Eötvös Loránd University
Institute of Mathematics

Ph.D. thesis

Directions and other topics in Galois-geometries

Marcella Takáts

Doctoral School: Mathematics
Director: Miklós Laczkovich
Professor, Member of the Hungarian Academy of Sciences

Doctoral Program: Pure Mathematics
Director: András Szűcs
Professor, Corresp. Member of the Hungarian Academy of Sciences

Supervisor: Péter Sziklai, D.Sc.
Associate Professor

Department of Computer Science
Institute of Mathematics
Eötvös Loránd University

2014

To the memory of Dr. Takáts Ágoston

Contents

Introduction

In this work we study geometries over finite fields (Galois-geometries), and "geometry style" properties of finite fields. The history of finite geometry goes back to the 1950s, to Benjamino Segre.

The two main ways of finite geometrical investigations are the combinatorial and the algebraic one. In both cases we define a point set by a combinatorial property, e.g. by its intersection numbers with certain subspaces. The first possibility is to examine what follows from the definition using combinatorial and geometrical tools. It is also common to rephrase the analogue of a question studied in classical Euclidean geometry.

The other way is the algebraic one. The connection between algebra and finite geometry is said to be classical (e.g. Mathieu-groups – Witt-designs). We take a point set in a geometry over a finite field and translate its "nice" combinatorial property to a "nice" algebraic structure. In the current thesis we mainly use the so-called polynomial method, developed by Blokhuis and Szőnyi. We assign a polynomial over a finite field to the point set, and examine the polynomial with various tools. We can study the coefficients of the polynomial, or its derivatives, or consider it as an algebraic curve. Then we translate the algebraic information we get back to the original, geometrical language.

Studying sets with a given (intersection) property often leads to spectrum results: we examine the possible sizes of the set, in particular the maximum or the minimum, and other specific information of the structure of the extremal (maximal or minimal) example.

Stability and extendability questions also arise: we consider structures with a given property and take an extremal one among them (e.g. the largest one), then we show that a structure close to it (in the sense of size) can be achieved only from the extremal one (by deleting some of its points).

In this work, which is based on six articles [1]-[6], we investigate combinatorial structures with purely combinatorial tools, mainly in Chapters 4, 5 and 6, and by algebraic methods in Chapters 1, 2 and 3.

The main part of the thesis is related to the so-called *direction problem*. Consider a point set in the affine space. We say a *direction* d is *determined* by the set if there is an affine line

with the ideal point d containing at least two points of the set. The investigated questions are the *number* of determined directions, and the characterization of the "interesting" point sets. A set is said to be "interesting" if there are only few determined directions. It is easy to see that in the n-dimensional space over a finite field of order q if the size of the set is greater than q^{n-1} then every direction is determined. So the maximal "interesting" size of a set is q^{n-1}. If the point set determines few directions only then we are interested in the *size* and the *structure* of the set. In fact, the most studied case is the maximal one, particularly in the plane, i. e. sets of cardinality q. This case was completely characterized by Blokhuis, Ball, Brouwer, Storme and Szőnyi in [15]. Point sets of smaller size are investigated as well. During these examinations stability questions also arose: the problem is whether we can add some points to such a set to reach a set of maximal cardinality such that the obtained set determines the same directions only.

In Chapter 2 we investigate the structure of point sets of non-maximal cardinality in the affine plane. We also study a stability question in projective spaces in Chapter 3. Finally, we introduce a natural generalization of the classical direction problem in higher dimensions in Chapter 4.

Chapter 2 is based on a joint work with Szabolcs Fancsali and Péter Sziklai. We prove a theorem about the number of directions determined by less then q affine points in the plane, similar to the result related to the extremal case of q points mentioned above. As these results have already appeared in [3] and also in the Ph.D. thesis of Szabolcs Fancsali [30], the current thesis contains a short summary of the topic; for the detailed description see [3] and [30].

The stability question we investigate in Chapter 3, based on [4], is the following. Given a point set of size $q^{n-1} - \varepsilon$ in an n-dimensional affine space, can we extend it to a set of size q^{n-1} such that the set of the determined directions remains the same. Earlier results contain conditions on the size of the set or on the size of the set of determined directions. Instead of following these methods we investigate the structure of the set of non-determined directions. We show that if ε is small then the set is typically extendable. If not, then the set of non-determined directions has a strong structure: it is contained in a plane curve of low degree. We describe an application in the theory of partial ovoids of certain generalized quadrangles.

In these two chapters we use efficient algebraic tools. These are nice illustrations of the polynomial method widely used in finite geometries. In the following chapter, which is the last one related to the direction problem, we turn to use purely geometrical considerations.

Chapter 4 gives a possible generalization of the direction problem, based on [2]. Consider a point set in the n-dimensional affine space over the finite field of q elements and let

$0 \leq k \leq n-2$. We extend the definition of *determined directions* in the following way: a k-dimensional subspace at infinity is *determined* by the set if there is an affine $(k+1)$-dimensional subspace through it which contains at least $k+2$ linearly independent points of the set (i. e. the points of the set spans this $(k+1)$-dimensional subspace). It turns out that the maximal size of an "interesting" point set is again q^{n-1}. We examine sets of this extremal size, and in certain cases we classify point sets *not* determining every k-subspace.

Chapter 1 is about Vandermonde and super-Vandermonde sets, based on [1]. Vandermonde sets were first defined by Gács and Weiner in [33]. Although the concept looks like purely algebraic, and it is interesting enough from the "finite fields point of view", Vandermonde sets play a role in finite geometry which is not yet completely explored. In this chapter we list the basic properties of Vandermonde sets, then we show the geometric connections. In Section 1.2 we classify the "small" and the "large" (super-)Vandermonde sets as multiplicative subgroups of the field.

In the last two chapters we show some connections of finite geometries with other areas of combinatorics. We describe a question related to graph theory and a combinatorial search problem.

In Chapter 5 we examine finite projective planes from a graph theoretical point of view, considering their incidence graphs, suggested by R. Bailey and P. Cameron. In a graph $\Gamma = (V, E)$ a vertex v is *resolved* by a vertex-set $S = \{v_1, \ldots, v_n\}$ if its (ordered) distance list with respect to S, $(d(v, v_1), \ldots, d(v, v_n))$, is unique. A set $A \subset V$ is resolved by S if all its elements are resolved by S. S is a *resolving set* in Γ if it resolves V. The *metric dimension of* Γ is the size of the smallest resolving set in it. In a bipartite graph a *semi-resolving set* is a set of vertices in one of the vertex classes that resolves the other class. We show that the metric dimension of the incidence graph of a finite projective plane of order $q \geq 23$ is $4q-4$, and describe all resolving sets of that size. This is a joint work with Tamás Héger. In this thesis, we have the focus on resolving sets. For the details of the case of semi-resolving sets, see [5] and the Ph.D. thesis of Tamás Héger [35].

In Chapter 6, which is based on [6], we consider the following q-analog of the basic combinatorial search problem: let q be a prime power, let V denote an n-dimensional vector space over the finite field of q elements and let $\mathbf{v}$ be an unknown 1-dimensional subspace of V. We will be interested in determining the minimum number of queries that is needed to find $\mathbf{v}$ provided all queries are subspaces of V and the answer to a query U is YES if $\mathbf{v} \leqslant U$ and NO if $\mathbf{v} \not\leqslant U$. We consider the adaptive case (when for each queries answers are obtained immediately and later queries might depend on previous answers) and the non-adaptive case (when all queries must be made at the same time). It turns out that differently from the classical search problem, the minimum numbers of queries are not the same in the

two cases. In three dimensions $2q-1$ queries are necessary and sufficient in the adaptive case, but it is not enough in the non-adaptive case. We also give bounds in general dimension.

Acknowledgements.

First of all, I am most grateful to my supervisor Péter Sziklai. After he had given me the first experience in doing research under my M.Sc. years, he taught me finite geometries carefully and guided my research solicitously, giving always a close attention to my work. I owe him the largest debt for all sorts of support.

I am greatly thankful to Tamás Szőnyi. The finite geometry group at ELTE has been growing around him, and the mathematical career of many is unimaginable without him. He takes an incredible care of the professional development in mathematics of his disciples, including me.

I would like to give special thanks to Tamás Héger, my roommate at ELTE for the warm, merry and inspiring atmosphere and for his inconceivable helpfulness.

I thank my coauthors Szabolcs L. Fancsali, Jan De Beule, Tamás Héger and Balázs Patkós for the experience of the joint work.

I am also thankful to Péter Csikvári and Zoltán L. Nagy from whom I learned a lot and who were always ready to help me.

I express my gratitude to Leo Storme and Jan De Beule for their hospitality and support during my visits in Ghent.

I am very much grateful to my family, especially to my father who showed me the love of maths and enthusiasm about solving problems for the first time. I wish to thank my husband and my parents for their support and care as they made possible for me to write this thesis.

My work was funded by the Hungarian National Foundation for Scientific Research (OTKA) grant K 81310.

Preliminaries

In this chapter we give a summary of the fundamentals, the necessary basic knowledge and the convention of notation we follow in the thesis. Possible general references here are [36] and [39].

0.1 Notation and basic definitions.

Throughout the whole thesis, let p be a prime, $q = p^h$ be a prime power, and let GF(q) be a finite field of q elements. We denote the elements of a field by lower case letters, while variables in an expression are denoted by capital letters.

Definition 0.1 (Projective plane). $\Pi = (\mathcal{P}, \mathcal{L}, I)$, where $\mathcal{P}$ and $\mathcal{L}$ are disjoint sets and I is an incidence relation, is a *projective plane*, if the following axioms hold:
P1 For any two $P_1, P_2 \in \mathcal{P}$ there exists exactly one $\ell \in \mathcal{L}$ which is incident with both P_1 and P_2.
P1' For any two $\ell_1, \ell_2 \in \mathcal{L}$ there exists exactly one $P \in \mathcal{P}$ which is incident with both ℓ_1 and ℓ_2.
P2 Any $\ell \in \mathcal{L}$ is incident with at least three elements of $\mathcal{P}$.
P2'Any $P \in \mathcal{P}$ is incident with at least three elements of $\mathcal{L}$.

We call the elements of the sets $\mathcal{P}$ and $\mathcal{L}$ points and lines, respectively, and I is incidence. If a point and a line are incident, we often write phrases like "a line contains a point" or "a line through a point".

Proposition 0.2. *If there is a line in the projective plane* Π *that contains* $n+1$ *points, then*

- *Every line in* Π *contains* $n+1$ *points.*
- *There are* $n+1$ *lines through any point of* Π.
- Π *contains* n^2+n+1 *points and* n^2+n+1 *lines.*

Definition 0.3. The *order* of the projective plane Π is n, if the lines in Π contain $n+1$ points.

For a projective plane we use the notation $\Pi = (\mathcal{P}, \mathcal{L})$ also (mainly in Chapter 5 when we focus on the sets of points or lines of the plane), while sometimes Π_n refers to a projective plane of order n (defined as above).

Definition 0.4 (Affine plane)**.** $\mathcal{A} = (\mathcal{P}', \mathcal{L}', I')$, where $\mathcal{P}'$ and $\mathcal{L}'$ are disjoint sets and I' is an incidence relation, is an *affine plane*, if the following axioms hold:
A1 For any two $P_1, P_2 \in \mathcal{P}'$ there exists exactly one $\ell \in \mathcal{L}'$ which is incident with both P_1 and P_2.
A1' If $P \in \mathcal{P}'$ is not incident with $\ell \in \mathcal{L}'$ then there exists exactly one $\ell' \in \mathcal{L}'$ which is incident with P but not with any of those elements of $\mathcal{P}'$ who are incident with ℓ.
A2 Any $\ell \in \mathcal{L}'$ is incident with at least two elements of $\mathcal{P}'$.
A2'Any $P \in \mathcal{P}'$ is incident with at least three elements of $\mathcal{L}'$.

We call the elements of the sets $\mathcal{P}'$ and $\mathcal{L}'$ points and lines, respectively, and I' is incidence.

Clearly, if we delete a line (and all its points) from a projective plane, we get an affine plane. It is easy to see that by adding $n+1$ suitable ideal points and one ideal line to an affine plane we get a projective plane.

Proposition 0.5. *If there is a line in the affine plane $\mathcal{A}$ that contains n points, then*

- *Every line in $\mathcal{A}$ contains n points.*
- *There are $n+1$ lines through any point of $\mathcal{A}$.*
- *$\mathcal{A}$ contains n^2 points and n^2+n lines.*

In Chapter 5 and partially in Chapter 6 we consider projective planes in general, defined only in combinatorial way as above. For some orders there exist many non-isomorphic projective planes. In the other chapters we work with projective planes (or spaces) over finite fields. When we turn to higher dimensional projective spaces, we do not need the axiomatic definition as the only examples are the ones over finite fields.

Let $\mathrm{PG}(n,q)$ denote the projective space of dimension n over $\mathrm{GF}(q)$. We associate a point of the projective space with a homogeneous $(n+1)$-tuple in brackets. It means that $(x_0, x_1, \ldots, x_n)$, $x_i \in \mathrm{GF}(q)$ refers to a point; $(x_0, x_1, \ldots, x_n)$ and $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$, $\lambda \in \mathrm{GF}(q)$ represent the same point; $(x_0, x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)$. Similarly, a homogeneous $(n+1)$-tuple in square brackets, $[y_0, y_1, \ldots, y_n]$, $y_i \in \mathrm{GF}(q)$, refers to a hyperplane. A point

is incident with a given hyperplane if and only if their scalar product $x_0y_0+x_1y_1+\cdots+x_ny_n$ is equal to zero.

Let $\mathrm{AG}(n,q)$ denote the affine space of dimension n over $\mathrm{GF}(q)$ that corresponds to the co-ordinate space $\mathrm{GF}(q)^n$ of rank n over $\mathrm{GF}(q)$. We can embed $\mathrm{AG}(n,q)$ into $\mathrm{PG}(n,q)$ in the usual way: then we think about $\mathrm{PG}(n,q)$ as $\mathrm{AG}(n,q)\cup H_\infty$, where H_∞ is called the *hyperplane at infinity* or the *ideal hyperplane*, and its points are called *ideal points* or *directions*. In case of $n=2$, the ideal hyperplane is simply called the *line at infinity* or the *ideal line*, denoted by ℓ_∞.

We choose the following co-ordinate system of $\mathrm{PG}(n,q)$: $H_\infty=[1,0,\ldots,0]$. Then the points of H_∞ are coordinatized as $(0,x_1,x_2,\ldots,x_n)$. The point $(0,\ldots,0,1)\in\ell_\infty$ is denoted by (∞), and it refers to the vertical direction. A point of $\mathrm{AG}(n,q)$ cannot have a zero in its first coordinate, thus, it can be written as $(1,x_1,x_2,\ldots,x_n)$.

A point $(1,x_1,x_2,\ldots,x_n)\in\mathrm{AG}(n,q)$ is also denoted by $(x_1,x_2,\ldots,x_n)$, written with *inhomogeneous* coordinates.

We use the terminology that for a fixed subset S of points of a projective space, a line ℓ is said to be *skew*, *tangent* or *secant* to S if $|\ell\cap S|=\emptyset$, 1 or $|\ell\cap S|\geq 2$ holds, respectively.

Now we define some special point sets of projective planes we will work with.

Definition 0.6. An *arc of degree d* of a projective plane Π of order s is a set $\mathcal{K}$ of points such that every line of Π meets $\mathcal{K}$ in at most d points. If $\mathcal{K}$ contains k points, than it is also called a $\{k,d\}$-arc. An arc $\mathcal{K}$ of degree d for which every secant line meets $\mathcal{K}$ in exactly d points, is called *maximal*.

Definition 0.7. An *oval* is a $\{q+1,2\}$-arc.

Definition 0.8. A *hyperoval* is a $\{q+2,2\}$-arc.

Through each point of an oval there is exactly one tangent line, while a hyperoval has not any tangent. The following theorem is essential in the theory of arcs.

Theorem 0.9 (Segre, [44])**.** *If q is odd, then all ovals of* $\mathrm{PG}(2,q)$ *are conics.*

In the last two chapters, where we examine some connections between finite geometries and other fields in combinatorics, we need further special point sets.

Definition 0.10. A set B of points is a *blocking set* in a projective plane Π, if $|B\cap\ell|\geq 1$ for any line $\ell\in\mathcal{L}$. A point P of a blocking set B is said to be *essential* if $B\setminus\{P\}$ is not a blocking set.

Definition 0.11. A set B of points is a *double blocking set* in a projective plane Π, if $|B\cap\ell|\geq 2$ for any line $\ell\in\mathcal{L}$. $\tau_2=\tau_2(\Pi)$ denotes the size of the smallest double blocking set in Π.

We need the definition of the incidence graph of a projective plane as well.

Definition 0.12. Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a projective plane with point set $\mathcal{P}$ and line set $\mathcal{L}$. The *incidence graph* $\Gamma(\Pi)$ of Π is a bipartite graph with vertex classes $\mathcal{P}$ and $\mathcal{L}$, where $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$ are adjacent in Γ if and only if P and ℓ are incident in Π.

0.2 The Rédei-polynomial

Now we introduce the main tool of the algebraic methods appearing in Chapters 2 and 3.

Let $U = \{(1, a_{i1}, a_{i2}, \ldots, a_{in}) : i = 1, ..., m\}$ be a point set in $\mathrm{AG}(n, q) \subset \mathrm{PG}(n, q)$. The Rédei-polynomial of U is defined as follows:

$R(X_0, X_1, X_2, ..., X_n) = \prod_{i=1}^{m}(X_0 + a_{i1}X_1 + a_{i2}X_2 + \cdots + a_{in}X_n)$.

This is clearly a totally reducible polynomial, where each linear factor corresponds to a point of U. Such a linear factor (called Rédei-factor) corresponding to a point $P = (1, a_1, a_2, \ldots, a_n)$ is $X_0 + a_1X_1 + a_2X_2 + \cdots + a_nX_n$. We substitute the *hyperplanes* of $\mathrm{PG}(n, q)$ into the polynomial. If the linear factor $X_0 + a_1X_1 + a_2X_2 + \cdots + a_nX_n$ is equal to zero when we substitute the hyperplane $[x_0, x_1, \ldots, x_n]$, then this hyperplane contains the point that corresponds to the linear factor. This is an equation of a hyperplane in the dual space $\mathrm{PG}(n, q)$. The points of this dual hyperplane correspond to such hyperplanes in the original space which go through the point $P = (1, a_1, a_2, \ldots, a_n)$.

Define the set $S(X_1, X_2, ..., X_n) = \{a_{i1}X_1 + a_{i2}X_2 + \cdots + a_{in}X_n : i = 1, ..., m\}$, then R can be written as

$$R(X_0, X_1, X_2, ..., X_n) = \sum_{j=0}^{m} \sigma_{m-j}(X_1, X_2, ..., X_n)X_0^j,$$

where $\sigma_j(X_1, X_2, ..., X_n)$ is the j-th elementary symmetric polynomial of the set $S(X_1, X_2, ..., X_n)$. R can be considered for a fixed $(X_1, X_2, ..., X_n) = (x_1, x_2, ..., x_n)$, then it is a univariate polynomial of X_0.

R can be considered as a hypersurface in the dual space $\mathrm{PG}(n, q)$. The points of R correspond to hyperplanes of the original space, where these hyperplanes intersect the point set. The hyperplane $[x_0, x_1, \ldots, x_n]$ contains exactly k points of U if and only if in the dual space $\mathrm{PG}(n, q)$, $(x_0, x_1, \ldots, x_n)$ is a point of the surface R with multiplicity k. Then the hyperplane $[x_0, x_1, \ldots, x_n]$ is a root of the polynomial $R(X_0, X_1, X_2, \ldots, X_n)$ with multiplicity k.

It means that the Rédei-polynomial contains the intersection properties of the set U with hyperplanes and translates them into algebraic properties. One may investigate the polynomial itself or the hypersurface defined by R in the dual space.

0.3 The direction problem

The largest part of this work is around the *direction problem*. Consider a point set U in the affine plane $\mathrm{AG}(2,q) \subset \mathrm{PG}(2,q)$. We say a *direction* d is *determined* by U if there is an affine line with the ideal point d containing at least two points of U.

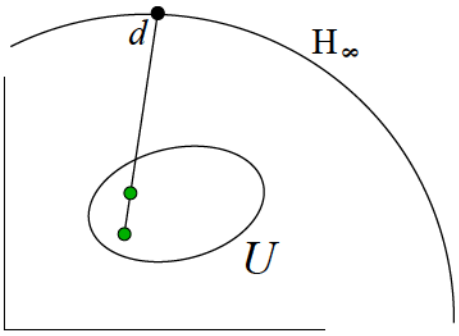

Figure 1: Direction determined by a point set.

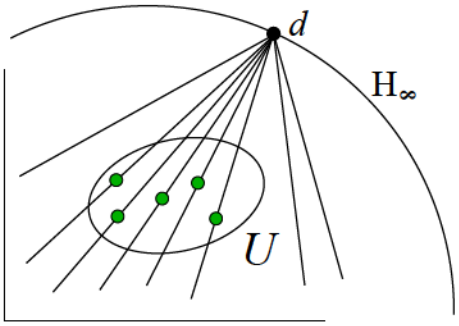

Figure 2: Non-determined direction.

Definition 0.13 (Direction set)**.** If U denotes an arbitrary set of points in the affine plane $\mathrm{AG}(2,q)$ then we say that the set

$$D = \left\{ \frac{b-d}{a-c} \;\middle|\; (a,b),(c,d) \in U, (a,b) \neq (c,d) \right\}$$

is the *set of directions determined by* U. We define $\frac{a}{0}$ as ∞ if $a \neq 0$, thus $D \subseteq \mathrm{GF}(q) \cup \{\infty\}$.

The original problem - due to Rédei - was stated for directions determined by the graph of a function in the plane over a finite field. Let $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ be a function and let $U = \{(x, f(x)) \mid x \in \mathrm{GF}(q)\} \subseteq \mathrm{AG}(2,q)$ be the graph of the function f. In this case $|U| = q$ and $\infty \notin D$.

It means that the "vertical" direction, i. e. the ideal point of the vertical lines is a *not determined direction.*

We can also formulate the definition in the n-dimensional space: Let U be a point set in the affine space $\mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$. We say a *direction* d is *determined* by U if there is an affine line with the ideal point d containing at least two points of U.

The question is that how many directions are determined by a point set and how the "interesting" point sets U look like. Here "interesting" means that there are only few determined directions. Note that in the n-dimensional space if $|U| > q^{n-1}$ then every direction is determined. One can prove it by the pigeon hole principle: take a point d on the hyperplane at infinity H_∞. There are q^{n-1} affine lines having d as their ideal point. If the cardinality of the set U is larger than q^{n-1} then at least one of the q^{n-1} lines will intersect U in at least two points, so d will be determined. This means that the extremal (maximal) "interesting" point sets are of size q^{n-1}.

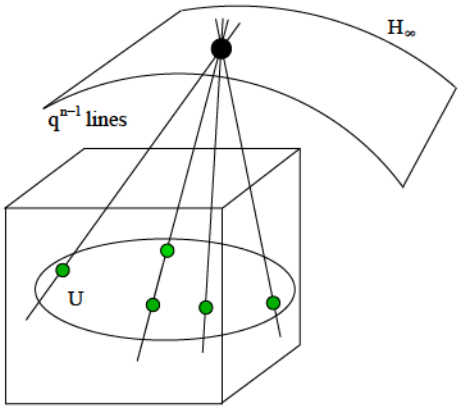

Figure 3: A set of cardinality larger than q^{n-1} determines every direction.

Note that already a random point set of size much less than q^{n-1} determines all the directions. There are several investigated questions concerning the direction problem. In fact, the $n = 2$ (planar) version is the most studied case. Considering maximal point sets (i. e. of size q) we can ask for the *number* of determined directions and the *structure* of a set as well if there are few determined directions. We can also formulate the same questions in case of sets of size less than q. The examination of such sets leads to stability questions as well: a set of size $q - \varepsilon$ whether can be extended to a set of size q determining the same directions only. The problems above are studied in general dimensions as well.

0.4 Results

Here we would like to give an outline of the known results due to the direction problem. Instead of giving a complete list of the existing theorems, we tried to choose some of the fundamental ones which seemed to be the most important from our point of view.

Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$ be a point set. Denote by D the set of directions determined by U, and by N the set of non-determined directions.

First we enlist some results in the planar case when the point set has the maximal (interesting) cardinality q. Let us begin with planes over fields of prime order.

Theorem 0.14 (Rédei-Megyesi, [43]). *Let U be a point set, $U \subseteq \mathrm{AG}(2,p)$, $|U| = p$, p prime. Then $|D| \geq \frac{p+3}{2}$ or U is contained in a line.*

Example. For q odd, let $A < \mathrm{GF}(q)^*$ be a multiplicative subgroup of index 2. Let $U = \{(a,0) : a \in A)\} \cup \{(0,a) : a \in A\} \cup \{(0,0)\}$. If $q = p$ prime, then the number of determined directions is $|D| = \frac{p+3}{2}$ which shows the sharpness of the bound above.

The following result shows that the point set determining exactly $\frac{p+3}{2}$ directions is unique.

Theorem 0.15 (Lovász-Schrijver, [40]). *Let $p > 2$ be a prime. If a point set $U \subset \mathrm{AG}(2,p)$, $|U| = p$ determines exactly $\frac{p+3}{2}$ directions, then (in a proper coordinate system) it can be written in the following form:*
$U = \{(a,0) : a \in A)\} \cup \{(0,a) : a \in A\} \cup \{(0,0)\}$, where $A < \mathrm{GF}(p)^*$ is a multiplicative subgroup of index 2.

Now we turn to planes of prime power order.

The following theorem gives the complete characterization of point sets of cardinality q.

Theorem 0.16 (Blokhuis-Ball-Brouwer-Storme-Szőnyi, [15], [11]). *Let $U \subset \mathrm{AG}(2,q)$ be a point set, $|U| = q$. Let $s = p^e$ be the largest power of p such that each secant meets U in a multiple of s points. Then one of the following holds:*
(i) $s = 1$ and $\frac{q+3}{2} \leq |D| \leq q+1$;
(ii) $\mathrm{GF}(s)$ is a subfield of $\mathrm{GF}(q)$ and $\frac{q}{s} + 1 \leq |D| \leq \frac{q-1}{s-1}$;
(iii) $s = q$ and $|D| = 1$.
If $s \geq 3$ then U is $\mathrm{GF}(s)$-linear.

Let us now consider point sets of non-maximal cardinality. First we recall a result on the number of determined directions in the prime case.

Theorem 0.17 (Szőnyi, [50]). *Let U be a point set, $U \subseteq \mathrm{AG}(2,p)$, p prime, $k \leq p$, $|U| = k$. Then $|D| \geq \frac{k+3}{2}$ or U is contained in a line.*

Example. Let $A < \mathrm{GF}(q)^*$ be a multiplicative subgroup of size $\frac{k-1}{2}$ (if it exists). Let $U = \{(a,0) : a \in A)\} \cup \{(0,a) : a \in A\} \cup \{(0,0)\}$. Then the number of determined directions is $|D| = \frac{k+3}{2}$, so this bound is also sharp.

We will be interested in extendability questions. We mention the following two results; however, the second theorem is a slight generalization of the first one.

Theorem 0.18 (Szőnyi, [49]). *Let $U \subset \mathrm{AG}(2,q)$ be a point set, $|U| = q - \varepsilon$. If $\varepsilon \leq \frac{\sqrt{q}}{2}$, $|D| \leq \frac{q+1}{2}$, then there exists $U_0 \subset \mathrm{AG}(2,q)$ such that $U \cap U_0 = \emptyset$, $|U_0| = \varepsilon$, and $U \cup U_0$ still determines D only.*

It has a "relaxed" version as well:

Theorem 0.19 (Sziklai, [47]). *Let $U \subset \mathrm{AG}(2,q)$ be a point set, $|U| = q - \varepsilon$, $\varepsilon \leq \alpha\sqrt{q}$, $|D| \leq (q+1)(1-\alpha)$, $\frac{1}{2} \leq \alpha \leq 1$. Then there exists $U_0 \subset \mathrm{AG}(2,q)$ such that $U \cap U_0 = \emptyset$, $|U_0| = \varepsilon$, and $U \cup U_0$ still determines D only.*

We finish this section with a stability result for general dimensions.

Theorem 0.20 (De Beule - Gács, Ball, [22], [12]). *Let $q = p^h$, p an odd prime and $h > 1$, and let $U \subseteq \mathrm{AG}(n,q)$, $n \geq 3$, be a set of affine points of size $q^{n-1} - 2$, which does not determine a set N of at least $p+2$ directions. Then U can be extended to a set of size q, not determining the set N of directions.*

Chapter 1

Vandermonde sets and super-Vandermonde sets

1.1 Introduction

The main part of this chapter was published in [1]. The introduction to the topic and the generalization are also based on [46]. The concept of Vandermonde sets was originally introduced by Gács and Weiner in [33].

Before we start to examine the main topic of this section, *Vandermonde sets* and *super-Vandermonde sets*, we recall some basic facts about symmetric polynomials. A polynomial $f(X_1, ..., X_n)$ is symmetric if $f(X_1, ..., X_n) = f(X_{\pi(1)}, ..., X_{\pi(n)})$ for any permutation π of $1, ..., n$.

Definition 1.1. The k-th elementary symmetric polynomial of variables $X_1, ..., X_n$ is

$$\sigma_k(X_1, ..., X_n) = \sum_{\{i_1,...,i_k\} \subseteq \{1,...,n\}} X_{i_1} X_{i_2} \cdots X_{i_k}$$

$\sigma_0 := 1$ and $\sigma_j := 0$ for $j > n$.

Definition 1.2. The k-th power sum of variables $X_1, ..., X_n$ is

$$\pi_k(X_1, ..., X_n) = \sum_{i=1}^{n} X_i^k.$$

The elementary symmetric polynomials of a set $S = \{s_1, s_2, \ldots, s_t\}$ from any field uniquely determine the set as

$$\sum_{i=0}^{t} \sigma_i(S) X^{t-i} = \prod_{j=1}^{t} (X + s_j).$$

The power sums not always determine the set. For a fixed k

$$\sum_{i=0}^{k} \binom{k}{i} \pi_i(S) X^{k-i} = \sum_{j=1}^{t} (X + s_j)^k.$$

In general we cannot get back the set S from this formula. The binomial coefficients may vanish, hiding π_i as well.

The Fundamental theorem of symmetric polynomials is the following:

Theorem 1.3. *Every symmetric polynomial can be expressed as a polynomial in the elementary symmetric polynomials.*

The so-called Newton formulae give the relations between π_k-s and σ_k-s, as the power sums, according to the Fundamental theorem, also can be expressed by elementary symmetric polynomials.

$$k\sigma_k = \pi_1\sigma_{k-1} - \pi_2\sigma_{k-2} + \ldots + (-1)^{i-1}\pi_i\sigma_{k-i} + \ldots + (-1)^{k-1}\pi_k\sigma_0$$

and

$$\pi_{t+k} - \pi_{t+k-1}\sigma_1 + \ldots + (-1)^i\pi_{t+k-i}\sigma_i + \ldots + (-1)^t\pi_k\sigma_t = 0$$

.

Define $\sigma_i = 0$ for any $i < 0$ or $i > t$, and for a fixed $k \geq 0$, $\pi_0 = k$. Then the two formulae can be generalized in the following form:

$$\sum_{i=0}^{k} (-1)^i \pi_i \sigma_{k-i} = 0$$

.

The use of Rédei-polynomials often leads to the examination of symmetric polynomials. Consider the affine Rédei-polynomial $R(X,Y) = \prod_i (X + a_iY + b_i)$. Expanding $R(X,Y)$ by X, the coefficients will be elementary symmetric polynomials: $\sigma_k(\{a_iY + b_i : i\})$.

Now we define an invariant. Let $S = \{x_1, ..., x_t\} \subseteq \mathrm{GF}(q)$ be a set of field elements, and $\pi_k = \pi_k(\{x_i : x_i \in S\}) = \sum_{x_i \in S} x_i^k$.

Let $w = w_S$ be the smallest positive integer k such that $\pi_k \neq 0$ if such a k exists, otherwise $w = \infty$.

Definition 1.4. Let $1 < t < q$. We say that $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$ is a *Vandermonde set*, if $\pi_k = \sum_i y_i^k = 0$ for all $1 \leq k \leq t-2$.

Here we do not allow multiple elements in T. Observe that the power sums do not change if the zero element is added to (or possibly removed from) T (but the cardinality

changes hence its "Vandermondeness" is weakened or strengthened). Note that in general the Vandermonde property is invariant under the transformations $y \to ay + b$ $(a \neq 0)$ if and only if $p \mid t$; if $p \not| t$ then a "constant term" tb^k occurs in the power sums.

Using the invariant $w = w_T$ we defined earlier, the Vandermonde property is equivalent to $w \geq t - 1$. In fact if $p \mid t$ then a t-set cannot have more than $t - 2$ zero power sums (so in this sense Vandermonde sets are extremal, with $w = t - 1$); this is an easy consequence of the fact that a Vandermonde determinant of distinct elements cannot be zero: consider the product

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ y_1 & y_2 & \dots & y_t \\ y_1^2 & y_2^2 & \dots & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & \dots & y_t^{t-1} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

it cannot result in the zero vector. (And the name "Vandermonde" comes from here.)

We note that if $1 < t \leq q$, $|T| = t$ and multiplicities are allowed then $w_T = \infty \Leftrightarrow$ all the multiplicities of the elements of T are divisible by the characteristic p.

The proof above, with slight modifications, shows that in general a t-set cannot have more than $t - 1$ zero power sums (so for a Vandermonde set w_T is either $t - 1$ or t). If the zero element does not occur in T then consider the product

$$\begin{pmatrix} y_1 & y_2 & \dots & y_t \\ y_1^2 & y_2^2 & \dots & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & \dots & y_t^{t-1} \\ y_1^t & y_2^t & \dots & y_t^t \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

it cannot result in the zero vector as the determinant is still non-zero. If $0 \in T$ then remove it: let $T^* = T \setminus \{0\}$. There are $t - 1$ elements in T^*, so we are again in the previous, zero-free situation: T^* cannot have more than $t - 2$ zero power sums. Adding 0 to T^*, the power sums do not change, so there will be at most $t - 2$ zero power sums in T.

Definition 1.5. Let $1 < t < q$. We say that $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$ is a *super-Vandermonde set*, if $\pi_k = \sum_i y_i^k = 0$ for all $1 \leq k \leq t - 1$.

So the super-Vandermonde property is equivalent to $w_T = t$. Note that the zero element is never contained in a super-Vandermonde set. (Suppose that T is a super-Vandermonde set containing the zero element and $|T| = t$. It has $t - 1$ zero power sums. Removing the

zero element the power sums do not change, so for the set of the other $t-1$ elements all the first $t-1$ power sums were zero, which is impossible according to the previous statement.) In fact *adding* the zero element to a super-Vandermonde set one gets a Vandermonde set, and same argument gives the first examples of super-Vandermonde sets:

Example 1.6. If T is a Vandermonde set, containing the zero element, then $T \setminus \{0\}$ is a super-Vandermonde set. In particular, if T is a Vandermonde set and $|T| = t$ is divisible by the characteristic p, then for any $a \in T$, the translate $T - a$ is a Vandermonde set, containing the zero element.

The same argument shows that if $|T| = t$ is a super-Vandermonde set then $p \not| t$.

In the next proposition we characterize the Vandermonde property.

Proposition 1.7. *Let $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$. The following are equivalent*

(i) T is a Vandermonde set, i.e. $w_T = t - 1$;

(ii) the polynomial $f(Y) = \prod_{i=1}^{t}(Y - y_i)$ is of the form $Y^{t'}g(Y)^p + aY + b$ (where $0 \leq t' \leq p-1$, $t' \equiv t \bmod p$);

(iii) for the polynomial $\chi(Y) = -\sum_{i=1}^{t}(Y - y_i)^{q-1}$, $tY^{q-1} + \chi(Y)$ has degree $q - t$; moreover

(iv) for some $Q = p^s$, $t - 1 \leq Q$, the polynomial $tY^{Q-1} - \sum_{i=1}^{t}(Y - y_i)^{Q-1}$ has degree $Q - t$.

Proof. The coefficients of χ are the power sums of the set T, so (i) and (iii) are clearly equivalent. (i) $\Leftrightarrow$(iv) is similar. The equivalence of (i) and (ii) is an easy consequence of the Newton formulae relating power sums and elementary symmetric polynomials. □

Note that for the function χ in (iii), $t + \chi(Y)$ is the characteristic function of T, that is it is 1 on T and 0 everywhere else. (ii) means that a Vandermonde set is equivalent to a *fully reducible* polynomial (i.e. it splits into linear factors) of form $g^p(Y) + Y^t + cY$. (In the important case when $p \mid t$ we have $g^p(Y) + Y$.)

In the next proposition we characterize the super-Vandermonde property.

Proposition 1.8. *Let $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$. The following are equivalent*

(i) T is a super-Vandermonde set, i.e. $w_T = t$;

(ii) the polynomial $f(Y) = \Pi_{i=1}^{t}(Y - y_i)$ is of the form $Y^{t'}g(Y)^p + c$ (where $0 \leq t' \leq p-1$, $t' \equiv t \bmod p$);

(iii) for the polynomial $\chi(Y) = -\sum_{i=1}^{t}(Y - y_i)^{q-1}$, $tY^{q-1} + \chi(Y)$ has degree $q - t - 1$; moreover

(iv) for some $Q = p^s$, $t \leq Q$, the polynomial $tY^{Q-1} - \sum_{i=1}^{t}(Y - y_i)^{Q-1}$ has degree $Q - t - 1$.

Proof. The proof is very similar to the Vandermonde case. The coefficients of χ are the power sums of the set T, so (i) and (iii) are clearly equivalent. (i) $\Leftrightarrow$(iv) is similar. The equivalence of (i) and (ii) is an easy consequence of the Newton formulae relating power sums and elementary symmetric polynomials. □

Now we give some examples for Vandermonde and super-Vandermonde sets.

Example 1.9. Let q be a prime power.

(i) Any additive subgroup of GF(q) is a Vandermonde set.

(ii) Any multiplicative subgroup of GF(q) is a super-Vandermonde set.

(iii) For q even, consider the points of AG$(2, q)$ as elements of GF(q^2). Any q-set corresponding to the affine part of a hyperoval (i.e. a set of $(q+2)$ points which is intersected by every line in 0 or 2 points) with two infinite points is a Vandermonde set in GF(q^2).

(iv) Let q be odd. Consider the points of AG$(2, q)$ as elements of GF(q^2) and a $(q+1)$-set $A = \{a_1, ..., a_{q+1}\}$ in it, intersecting every line in at most two points (i.e. an *oval* or $(q+1)$-arc). Suppose that it is in a normalized position, i.e. $\sum a_i = 0$. Then A is a super-Vandermonde set in GF(q^2).

Proof. (i) Suppose T is an additive subgroup of size t in GF(q). We want to prove that Proposition 1.7 (ii) is satisfied, that is $f(Y) = \Pi_{y \in T}(Y - y)$ has only terms of degree divisible by p, except for the term Y. By [36], Lemma 8.38 if we prove that f is additive, hence GF(p)-linear, then this implies that f has only terms of degree a power of p.

Consider the polynomial in two variables $F(X, Y) = f(X) + f(Y) - f(X + Y)$. First of all note that it has full degree at most t and that the coefficient of X^t and Y^t is zero. Considering F as a polynomial in X, we have

$$F(X, Y) = r_1(Y)X^{t-1} + r_2(Y)X^{t-2} + \cdots + r_t(Y),$$

where $r_i(Y)$ $(i = 1, \ldots t)$ is a polynomial in Y of degree at most i (and $\deg(r_t) \leq t - 1$). Now $F(X, y) \equiv 0$ for any $y \in T$ (as a polynomial of X), so all r_i-s have at least t roots. Since their degree is smaller than this number, they are zero identically, so we have $F(X, Y) \equiv 0$, hence f is additive.

(ii) Suppose T is a multiplicative subgroup of size t in GF(q). Then the polynomial $f(Y) = \Pi_{i \in T}(Y - y_i)$ is of the form $Y^t - 1$ so Proposition 1.8 (ii) is satisfied, we are done.

(iii) Let $\{x_1, ..., x_q\} \subseteq \mathrm{GF}(q^2)$ correspond to the affine part of the hyperoval $\mathcal{H}$ and ε_1 and ε_2 be $(q+1)$-st roots of unity corresponding to the two infinite points. Consider the polynomial $\chi(X) = \sum_{i=1}^{q}(X - x_i)^{q-1}$. For any point x out of the hyperoval every line through x meets $\mathcal{H}$ in an even number of points, and since $(x - x_i)^{q-1}$ represents the slope of the line joining the affine points x and x_i, we have that $\chi(x) = \varepsilon_1 + \varepsilon_2$ for any $x \notin \{x_1, ..., x_q\}$. There are $q^2 - q$ different choices for such an x, while the degree of χ is at most $q - 2$, so $\chi(X) \equiv \varepsilon_1 + \varepsilon_2$ identically (that is, all coefficients of χ are zero except for the constant term), so by Proposition 1.7 (iv), we are done.
(iv) A short proof is that by Segre's theorem such a point set is a conic if q is odd, so affine equivalent to the "unit circle" $\{\alpha \in \mathrm{GF}(q^2) : \alpha^{q+1} = 1\}$, which is a multiplicative subgroup. □

For a multiplicative subgroup $H = \langle\alpha\rangle \leq (\mathrm{GF}(q)^*, \cdot)$, $|H| = t$, its root polynomial is $\prod_{h\in H}(Y - h) = Y^t - 1$.

Note that Proposition 1.7 (iv) implies that if $T \subseteq \mathrm{GF}(q_1) \leq \mathrm{GF}(q_2)$ then T is a Vandermonde set in $\mathrm{GF}(q_1)$ if and only if it is a Vandermonde set in $\mathrm{GF}(q_2)$.

There are other interesting examples for super-Vandermonde sets as well.

Example 1.10. Let $q = q_0^{t-1}$, then in $\mathrm{GF}(q)$ let $T = \{1\} \cup \{\omega^{q_0^i} : i = 0, ..., t-2\}$ for some element $\omega \in \mathrm{GF}(q)^*$ satisfying $\mathrm{Tr}_{q\to q_0}(\omega^k) = -1$ for all $k = 1, ..., t-1$.

As:

$$\sum_{i=0}^{t-2}(\omega^{q_0^i})^k = \sum_{i=0}^{t-2}(\omega^k)^{q_0^i} = \mathrm{Tr}_{q\to q_0}(\omega^k) = -1.$$

We mention here without a proof that in a suitable field such an element ω exists.

Proposition 1.11. *Let $T = \{y_1, ..., y_t\}$ be a super-Vandermonde set. Then*

$$\left(\frac{y_1}{y_2} - 1\right)\left(\frac{y_1}{y_3} - 1\right)\cdots\left(\frac{y_1}{y_t} - 1\right) = t.$$

Proof. Consider the product

$$\begin{pmatrix} 1-t & 1 & ... & 1 \\ y_1 & y_2 & ... & y_t \\ y_1^2 & y_2^2 & ... & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & ... & y_t^{t-1} \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

it results in the zero vector since T is a super-Vandermonde set. It means that the determinant is zero, so

$$\begin{vmatrix} 1-t & 1 & ... & 1 \\ y_1 & y_2 & ... & y_t \\ y_1^2 & y_2^2 & ... & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & ... & y_t^{t-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & ... & 1 \\ y_1 & y_2 & ... & y_t \\ y_1^2 & y_2^2 & ... & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & ... & y_t^{t-1} \end{vmatrix} + \begin{vmatrix} -t & 0 & ... & 0 \\ y_1 & y_2 & ... & y_t \\ y_1^2 & y_2^2 & ... & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & ... & y_t^{t-1} \end{vmatrix} = 0.$$

The first term is the Vandermonde determinant of T. The second term can be expanded by the first row:

$$\begin{vmatrix} -t & 0 & ... & 0 \\ y_1 & y_2 & ... & y_t \\ y_1^2 & y_2^2 & ... & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & ... & y_t^{t-1} \end{vmatrix} = -t \begin{vmatrix} y_2 & y_3 & ... & y_t \\ y_2^2 & y_3^2 & ... & y_t^2 \\ \vdots & & & \\ y_2^{t-1} & y_3^{t-1} & ... & y_t^{t-1} \end{vmatrix} = -ty_2y_3...y_t \begin{vmatrix} 1 & 1 & ... & 1 \\ y_2 & y_3 & ... & y_t \\ y_2^2 & y_3^2 & ... & y_t^2 \\ \vdots & & & \\ y_2^{t-2} & y_3^{t-2} & ... & y_t^{t-2} \end{vmatrix},$$

we have got the Vandermonde determinant of $\{y_2, y_3, ..., y_t\}$. So

$VdM(y_1, y_2, ..., y_t) - ty_2y_3...y_tVdM(y_2, y_3, ..., y_t) = 0$, which means

$VdM(y_1, y_2, ..., y_t) = ty_2y_3...y_tVdM(y_2, y_3, ..., y_t)$, so

$$\frac{VdM(y_1, y_2, ..., y_t)}{y_2y_3...y_tVdM(y_2, y_3, ..., y_t)} = t.$$

Since the Vandermonde determinant is $VdM(y_1, y_2, ..., y_t) = \prod_{i<j}(y_i - y_j)$, we get

$$\frac{\prod_i(y_1 - y_i)}{y_2y_3...y_t} = t.$$

□

1.2 Small and large super-Vandermonde sets

If in Proposition 1.8(ii) we write $Y^t f(\frac{1}{Y})$ then we get a polynomial of degree t and its roots are $\{\frac{1}{y} : y \in T\}$. Hence a super-Vandermonde set is equivalent to a *fully reducible* polynomial of form $g^p(Y) + Y^t$, $t > p \cdot \deg g$.

Let's explore this situation. Firstly, if $q = p$ is a prime then the only possibility is $f(Y) = Y^t + c$, i.e. a transform of the multiplicative group $\{y : y^t = 1\}$, if it exists (so iff $t \mid q - 1$).

If q is not a prime, $f(Y) = g^p(Y) + Y^t$ is a fully reducible polynomial without multiple roots, so we can write it as $Y^q - Y = f(Y)h(Y)$. Then we may use the trick due to Gács:

differentiating this equation one gets

$$-1 = tY^{t-1}h(Y) + f(Y)h'(Y).$$

Substituting a root y_1 of f we get $h(y_1) = \frac{-1}{ty_1^{t-1}} = -\frac{1}{t}y_1^{q-t}$. Suppose that $t > \frac{q}{2}$, then $h(Y) = -\frac{1}{t}Y^{q-t}$ holds for more values than its degree hence it is a polynomial identity implying a contradiction unless $q - t = 1$. As $t = \frac{q}{2}$ is impossible (it would imply $p = 2$ and f would be a power), we have that either $t = q-1$ (and then $h(Y) = Y$ so $f(Y) = Y^{q-1} - 1$) or $t \leq \frac{q-1}{2}$.

For describing small and large super-Vandermonde sets we need to examine the coefficients of the original equation $Y^q - Y = f(Y)h(Y)$ carefully. What does small and large mean? We know that any additive subgroup of GF(q) forms a Vandermonde set, so removing the zero element from it one gets a super-Vandermonde set. The smallest and largest non-trivial additive subgroups are of cardinality p and q/p, respectively. This motivates that, for our purposes small and large will mean "of size $< p$" and "of size $> q/p$", resp. Note that the super-Vandermonde set, derived from an additive subgroup of size p, is a transform of a multiplicative subgroup. This does not hold for the super-Vandermonde set got from an additive subgroup of size q/p.

Theorem 1.12. *Suppose that $T \subset$ GF(q) is a super-Vandermonde set of size $|T| < p$. Then T is a (transform of a) multiplicative subgroup.*

Proof. Let $t = |T|$. Since $t < p$ the polynomial $f(Y)$ is of the form

$f(Y) = Y^t - b_0$.

If Y is a root of the equation then

$Y^t = b_0$.

It means that b_0 is a t-power. Let s be the *g.c.d.* of t and $q-1$. The number of the t-powers is $\frac{q-1}{s}$. It means that we can get any of them from s elements as their t-powers.
Since $f(Y)$ is a fully reducible polynomial without multiple roots, it has t different roots, equivalently, b_0 has precisely t distinct t-th roots. Hence $s = t$, which implies $t \mid q-1$.
Hence if $t < p$, it is true that $t \mid q-1$ so $t = \frac{q-1}{n}$, which means T is a coset of a multiplicative subgroup. □

Our main result in the current chapter is the characterization of small and large super-Vandermonde sets. Although the proof of Theorem 1.12 was short and simple, the classification of large super-Vandermonde sets turned out to be much more complicated. We describe it in the proof of the following theorem.

Theorem 1.13. *Suppose that $T \subset$ GF(q) is a super-Vandermonde set of size $|T| > q/p$. Then T is a (transform of a) multiplicative subgroup.*

Proof. Let $t = |T|$. Let

$f(Y) = Y^t + b_{mp}Y^{mp} + b_{(m-1)p}Y^{(m-1)p} + ... + b_pY^p + b_0$

and

$h(Y) = Y^{q-t} + a_{q-t-1}Y^{q-t-1} + ... + a_2Y^2 + a_1Y$

such that

$$Y^q - Y = f(Y)h(Y)$$

Substituting f and h we get

$$Y^q - Y = (Y^t + b_{mp}Y^{mp} + b_{(m-1)p}Y^{(m-1)p} + ... + b_pY^p + b_0)(Y^{q-t} + a_{q-t-1}Y^{q-t-1} + ... + a_2Y^2 + a_1Y)$$

The main concept of the proof is the careful examination of the coefficients appearing in the right hand side of this equation.

Let n be defined as $n := \lceil \frac{q-1}{t} \rceil$.

Consider the coefficient of $Y^1, Y^2, ..., Y^q$ in the previous equation. We get

Y^1 : $\quad -1 = a_1b_0$

Y^j : $\quad a_j = 0$ if $2 \leq j \leq t$ and $j \neq 1 \pmod p$

Y^j : $\quad a_j = 0$ if $t+1 \leq j \leq 2t$ and $j \neq 1, t+1 \pmod p$

Y^j : $\quad a_j = 0$ if $2t+1 \leq j \leq 3t$ and $j \neq 1, t+1, 2t+1 \pmod p$

and so on, generally

Y^j : $\quad a_j = 0$ if $kt+1 \leq j \leq (k+1)t$ and $j \neq 1, t+1, ..., kt+1 \pmod p$.

Y^{p+1} : $\quad a_{p+1}b_0 + a_1b_p = 0$

Y^{2p+1} : $\quad a_{2p+1}b_0 + a_{p+1}b_p + a_1b_{2p} = 0$

generally

Y^{kp+1} : $\quad a_{kp+1}b_0 + a_{(k-1)p+1}b_p + ... + a_{p+1}b_{(k-1)p} + a_1b_{kp} = 0,$

for $k = 1, 2, ..., m$.

Y^{t+1} : $\quad a_1 + b_0a_{t+1} + b_pa_{t-p+1} + b_{2p}a_{t-2p+1} + ... + b_{mp}a_{t-mp+1} = 0.$

The indices j of coefficients a_j are of the form $t-kp+1$. Since $t-kp+1 < t$ and $t-kp+1 \neq 1 \pmod p$ (because $t \neq 0 \pmod p$ is true) these coefficients are 0.

So the equation is of the form

Y^{t+1} : $\quad a_1 + b_0a_{t+1} = 0.$

Y^{2t+1} : $\quad a_{t+1} + b_0a_{2t+1} + b_pa_{2t-p+1} + ... + b_{mp}a_{2t-mp+1} = 0.$

The indices j of coefficients a_j are $t < j < 2t$. These coefficients are 0 if $j \neq 1, t+1 \pmod p$. It means $2t+1 \neq 1 \pmod p$ so $2t \neq 0 \pmod p$, which means $p \neq 2$. The other condition $2t+1 \neq t+1 \pmod p$ is satisfied by any t. Hence

Y^{2t+1} : $\quad a_{t+1} + b_0a_{2t+1} = 0$ if $p \neq 2$.

Similarly

Y^{3t+1} : $a_{2t+1} + b_0 a_{3t+1} + b_p a_{3t-p+1} + ... + b_{mp} a_{3t-mp+1} = 0.$

The indices are between $2t$ and $3t$ here. The coefficients are 0 if $3t+1 \neq 1, t+1, 2t+1 \pmod p$. It gives only one new condition: $3t+1 \neq 1 \pmod p$ so $3t \neq 0 \pmod p$ which means $p \neq 3$. The two other conditions have occurred earlier: $p \neq 2$ and $t \neq 0 \pmod p$.

Y^{3t+1} : $a_{2t+1} + b_0 a_{3t+1} = 0$ if $p \neq 2, 3$.

Generally

Y^{lt+1} : $a_{(l-1)t+1} + b_0 a_{lt+1} + b_p a_{lt-p+1} + ... + b_{mp} a_{lt-mp+1} = 0,$

for $l = 1, 2, ..., n-1$.

The indices are of the form $t - kp + 1$ and they are between $(l-1)t$ and lt. Hence the coefficients a_j are 0 if $lt+1 \neq 1, t+1, ..., (l-1)t+1 \pmod p$. It gives $(l-1)t$ conditions:

$lt+1 \neq 1 \pmod p$ so $p \neq l$;

$lt+1 \neq t+1 \pmod p$ so $p \neq (l-1)$;

$lt+1 \neq 2t+1 \pmod p$ so $p \neq (l-2)$;

and so on

$lt+1 \neq (l-2)t+1 \pmod p$ so $p \neq 2$;

finally

$lt+1 \neq (l-1)t+1 \pmod p$ so $t \neq 0$, which is true.

Hence generally we get

Y^{lt+1} : $a_{(l-1)t+1} + b_0 a_{lt+1} = 0$ if $p \neq 1, 2, ..., l$.

In particular, substituting $l = n-1$ into this equation we get

$Y^{(n-1)t+1}$: $a_{(n-2)t+1} + b_0 a_{(n-1)t+1} = 0$ if $p \neq 1, 2, ..., n-1$.

The greatest index j of a coefficient a_j can be $q - t - 1$.

$(n-1)t < q-1$ and $nt \geq q-1$ because of the definition of n.

It means that $(n-1)t \geq q - t - 1$ so $(n-1)t + 1 \geq q - t$.

It implies that $a_{(n-1)t+1}$ (which occurred in the previous equation) does not exist.

So we have two possibilities:

Case 1. $(n-1)t + 1 = q - t$, so the equation is of the form

$Y^{(n-1)t+1}$: $a_{(n-2)t+1} + b_0 = 0.$

Case 2. $(n-1)t + 1 > q - t$, so the equation is of the form

$Y^{(n-1)t+1}$: $a_{(n-2)t+1} = 0$ if $p \neq 1, 2, ..., n-1$.

We will prove that **Case 2** leads to a contradiction.

Case 1. $(n-1)t + 1 = q - t$ so $t = \frac{q-1}{n}$.

In that case, we can write 1 instead of $a_{(n-1)t+1}$.

Case 2. $a_{(n-2)t+1} = 0$.

Substituting this into the equation

$Y^{(n-2)t+1}$: $a_{(n-3)t+1} + b_0 a_{(n-2)t+1} = 0$, we get $a_{(n-3)t+1} = 0$.

We can substitute this again into the equation

$Y^{(n-3)t+1}$: $a_{(n-4)t+1} + b_0 a_{(n-3)t+1} = 0$, and we get $a_{(n-4)t+1} = 0$.

Substituting this in a decreasing order we get

Y^{t+1} : $a_1 + b_0 a_{t+1} = 0$ so $a_1 = 0$.

Hence $-1 = a_1 b_0$, so $a_1 \neq 0$, **Case 2** implied a contradiction.

It means that **Case 1** will occur, so $t = \frac{q-1}{n}$ if $p \neq 1, 2, ..., n-1$.

In other words $t \mid q-1$ if $p \neq 1, 2, ..., n-1$.

Hereafter, we can write 1 instead of a_j if $j = (n-1)t + 1$,

and 0 if $j > (n-1)t + 1$.

$Y^{(n-1)t+1}$: $a_{(n-2)t+1} + b_0 = 0$ so $a_{(n-2)t+1} = -b_0$.

Substituting this into the equation

$Y^{(n-2)t+1}$: $a_{(n-3)t+1} + b_0 a_{(n-2)t+1} = 0$, we get

$Y^{(n-2)t+1}$: $a_{(n-3)t+1} + b_0 b_0 = 0$ so $a_{(n-3)t+1} = {b_0}^2$.

Substituting this in a decreasing order we get

Y^{lt+1} : $a_{(l-1)t+1} = (-b_0)^{n-l}$ for $l = n-1, n-2, ..., 1$.

Finally

Y^{t+1} : $a_1 = (-b_0)^{n-1}$.

Substituting this into the equation $-1 = a_1 b_0$, we get $-1 = (-b_0)^{n-1} b_0$ so $1 = (-b_0)^n$.

We follow the examination of the coefficients with the terms of the form $Y^{lt+kp+1}$:

$Y^{(n-1)t+p+1}$: $a_{(n-2)t+p+1} + b_p + b_{2p} a_{(n-1)t+p+1} + ... = 0$

We have already seen that the coefficients a_j occurring in this equation are 0, because these are the same as in the equation of $Y^{(n-1)t+1}$. So

$Y^{(n-1)t+p+1}$: $a_{(n-2)t+p+1} + b_p = 0$.

Similarly

$Y^{(n-1)t+2p+1}$: $a_{(n-2)t+2p+1} + b_{2p} = 0$,

generally

$Y^{(n-1)t+kp+1}$: $a_{(n-2)t+kp+1} + b_{kp} = 0$ for $k = 1, 2, ..., m$.

On the other hand

Y^{lt+p+1} : $a_{(l-1)t+p+1} + b_0 a_{lt+p+1} + b_p a_{lt+1} = 0$ for $l = 1, 2, ..., n-1$.

Generally we get

$Y^{lt+kp+1}$: $a_{(l-1)t+kp+1} + b_0 a_{lt+kp+1} + b_p a_{lt+(k-1)p+1} + ... + b_{kp} a_{lt+1} = 0$

for $l = 1, 2, ..., n-1$ and $k = 1, 2, ..., m$.

Particularly, if $l = 1$ the equation is of the form

Y^{t+kp+1} : $a_{kp+1} + b_0 a_{t+kp+1} + b_p a_{t+(k-1)p+1} + ... + b_{kp} a_{t+1} = 0$.

Lemma 1.14. $b_p = b_{2p} = ... = b_{mp} = 0$.

Proof of Lemma 1.14. We prove it by induction.

First we show that $b_p = 0$.

Consider the equation

$$Y^{(n-2)t+p+1}: \quad a_{(n-3)t+p+1} + b_0 a_{(n-2)t+p+1} + b_p a_{(n-2)t+1} = 0. \qquad (*)$$

We have seen that

$$Y^{(n-1)t+p+1}: \quad a_{(n-2)t+p+1} + b_p = 0 \text{ so } a_{(n-2)t+p+1} = -b_p$$

and

$$Y^{(n-1)t+1}: \quad a_{(n-2)t+1} = -b_0.$$

Substituting these into the equation $(*)$, we get

$$Y^{(n-2)t+p+1}: \quad a_{(n-3)t+p+1} - b_0 b_p - b_0 b_p - b_0 = 0 \text{ so } a_{(n-3)t+p+1} = 2b_0 b_p.$$

Generally we can write

$$Y^{lt+p+1}: \quad a_{(l-1)t+p+1} + b_0 a_{lt+p+1} + b_p a_{lt+1} = 0 \text{ for } l = n-1, n-2, ..., 1. \qquad (**)$$

Substituting

$$Y^{(l+1)t+p+1}: \quad a_{lt+p+1} = (-1)^{n-l-1}(n-l-1)b_0^{n-l-2}b_p$$

and

$$Y^{(l+1)t+1}: \quad a_{lt+1} = (-b_0)^{n-l-1}$$

into the equation $(**)$, we get

$$Y^{lt+p+1}: \quad a_{(l-1)t+p+1} = (-1)^{n-l}(n-l)b_0^{n-l-1}b_p \text{ for } l = n-1, n-2, ..., 1.$$

If $l = 0$ it means

$$Y^{p+1}: \quad a_{p+1}b_0 + a_1 b_p = 0. \qquad (***)$$

Substituting

$$Y^{t+p+1}: \quad a_{p+1} = (-1)^{n-1}(n-1)b_0^{n-2}b_p$$

and

$$Y^{t+1}: \quad a_1 = (-b_0)^{n-1}$$

into $(***)$, we get

$$Y^{p+1}: \quad (-1)^{n-1} n b_0^{n-1} b_p = 0.$$

In this equation $-1 \neq 0 \pmod p$, $n \neq 0 \pmod p$ and $b_0 \neq 0 \pmod p$ (from the equation $a_1 b_0 = -1$). It means that $b_p = 0$.

Now suppose that $b_p = b_{2p} = ... = b_{(s-1)p} = 0$.

We show that this implies $b_{sp} = 0$.

Consider the equation

$$Y^{(n-2)t+sp+1}: \quad a_{(n-3)t+sp+1} + b_0 a_{(n-2)t+sp+1} + b_{sp} a_{(n-2)t+1} = 0. \qquad (\star)$$

We have seen that

$$Y^{(n-1)t+sp+1}: \quad a_{(n-2)t+sp+1} + b_{sp} = 0 \text{ so } a_{(n-2)t+sp+1} = -b_{sp}$$

and

$$Y^{(n-1)t+1}: \quad a_{(n-2)t+1} = -b_0.$$

Substituting these into the equation $(\star)$, we get

$Y^{(n-2)t+sp+1}$: $\quad a_{(n-3)t+sp+1} - b_0 b_{sp} - b_0 b_{sp} = 0$ so $a_{(n-3)t+sp+1} = 2b_0 b_{sp}$.

Generally we can write

$Y^{lt+sp+1}$: $\quad a_{(l-1)t+sp+1} + b_0 a_{lt+sp+1} + b_{sp} a_{lt+1} = 0$ for $l = n-1, n-2, ..., 1.$ $\qquad (\star\star)$

Substituting

$Y^{(l+1)t+sp+1}$: $\quad a_{lt+sp+1} = (-1)^{n-l-1}(n-l-1)b_0^{n-l-2} b_{sp}$

and

$Y^{(l+1)t+1}$: $\quad a_{lt+1} = (-b_0)^{n-l-1}$

into the equation $(\star\star)$, we get

$Y^{lt+sp+1}$: $\quad a_{(l-1)t+sp+1} = (-1)^{n-l}(n-l)b_0^{n-l-1} b_{sp}$ for $l = n-1, n-2, ..., 1.$

If $l = 0$ it means

Y^{sp+1} : $\quad a_{sp+1} b_0 + a_1 b_{sp} = 0.$ $\qquad (\star\star\star)$

Substituting

Y^{t+sp+1} : $\quad a_{sp+1} = (-1)^{n-1}(n-1)b_0^{n-2} b_{sp}$

and

Y^{t+1} : $\quad a_1 = (-b_0)^{n-1}$

into $(\star\star\star)$, we get

Y^{sp+1} : $\quad (-1)^{n-1} n b_0^{n-1} b_{sp} = 0.$

In this equation $-1 \neq 0 \pmod p$, $n \neq 0 \pmod p$ and $b \neq 0 \pmod p$ (from the equation $a_1 b_0 = -1$). It means that $b_{sp} = 0$. ■

So we have got $b_p = b_{2p} = ... = b_{mp} = 0$. It means that $f(Y)$ is of the form

$f(Y) = Y^t + b_0,$

and we also get that $t \mid q-1$ so $t = \frac{q-1}{n}$ and $(-b_0)^n = 1$.

It means that

$f(Y) = Y^{\frac{q-1}{n}} + b_0$, where $(-b_0)^n = 1$ if $p \neq 1, 2, ..., n-1 \pmod p$.

So the roots of $f(Y)$ are the elements of a coset of a multiplicative subgroup of order t.

□

Consider $q = p^2$. There are two cases: $n > p$ or $n < p$. If $n > p$ then $t < p$ because of the definition of n, it is a "small super-Vandermonde set". If $n < p$ then $t > p$, it is a "large super-Vandermonde set", and $n < p$ is the condition of the theorem. It means that we classified that case: if $q = p^2$ then a super-Vandermonde set of $GF(q)$ is a coset of a multiplicative subgroup.

1.3 Final remarks

Many interesting point sets have constant intersection numbers $\mod p$ with lines (small blocking sets, unitals, maximal arcs). We may give them the name generalized Vandermonde sets. Here we refer to [46].

Theorem 1.15 (Sziklai, [46]). *Given a point set* $S = \{(a_i, b_i, c_i), i = 1, ..., s\} = \{(a_i, b_i, 1) : i = 1, ...s_1\} \cup \{(a_j, b_j, 0) : j = s_1 + 1, ..., s\} \subseteq \mathrm{PG}(2, q)$, *the following are equivalent:*

(i) S *intersects each line in* $r \mod p$ *points for some fixed* r*;*

(ii) $G(X, Y, Z) = \sum_{i=1}^{|S|}(a_iX + b_iY + c_iZ)^{q-1} \equiv 0$*;*

(iii) for all $0 \leq k + l \leq q - 1$, $\binom{k+l}{k} \neq 0 \mod p$, *we have* $\sum_{i=1}^{|S|} a_i^{q-1-k-l} b_i^k c_i^l = 0$*;*

(iv) for all $0 \leq k + l \leq q - 2$, $\binom{k+l}{k} \neq 0 \mod p$, *we have* $\sum_{i=1}^{s_1} a_i^k b_i^l = 0$ *and for all* $0 \leq m \leq q - 1$, $\sum_{i=1}^{s} a_i^{q-1-m} b_i^m = 0$.

□

Take the "affine" part of a Vandermonde set, i. e. points with $c_i \neq 0$, and write all its points in the form $(a_i, b_i, 1)$. Identify $\mathrm{AG}(2, q)$ with $\mathrm{GF}(q^2)$ then a point becomes $a_i + b_i\omega$ for some generator ω of $\mathrm{GF}(q^2)$. Substituting $(1, \omega, Z)$ into G we get

$0 = G(1, \omega, Z) = \sum_{(a_i,b_i,1)\in S}((a_i + b_i\omega) + Z)^{q-1} + \sum_{(a_j,b_j,0)\in S}(a_j + b_j\omega)^{q-1} =$

$= \sum_{k=0}^{q-2} \pm Z^{q-1-k} \sum_{(a_i,b_i,1)\in S}(a_i + b_i\omega)^k + \sum_{(a_i,b_i,c_i)\in S}(a_i + b_i\omega)^{q-1}$

which means that the affine part of a (generalized) Vandermonde set, considered as a set in $\mathrm{GF}(q^2)$, has power sums equal to zero for exponents $1, ..., q - 2$. (The last, constant term, is just $G(1, \omega, 0) = 0$.)

Chapter 2

The number of directions determined by less than q points

2.1 Introduction

This chapter is based on a joint work with Szabolcs Fancsali and Péter Sziklai. These results have already appeared in [3] and also in the Ph.D. thesis of Szabolcs Fancsali [30]. As that is an earlier, accepted work of Szabolcs Fancsali, here we just give a short summary of the topic; the method and the results. For the detailed description see [3] and [30]. Nevertheless, I did not want to miss it out totally, as it fits into the main topic of the current thesis, among the different versions and extensions of the direction problem, and, in particular, it is a nice illustration of the use of algebraic (polynomial) methods in finite geometry.

Notation.

- In this chapter, $\mathbb{F}$ denotes an arbitrary field (or maybe a Euclidean ring).
- Let $\mathcal{U}$ denote an affine point set, so $\mathcal{U} \subseteq \mathrm{AG}(2,q)$.
- Let $\mathcal{D}$ denote the set of directions determined by the point set $\mathcal{U}$.

Let us recall the original problem of direction sets. Let $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ be a function and let $\mathcal{U} = \{(x, f(x)) \mid x \in \mathrm{GF}(q)\} \subseteq \mathrm{AG}(2,q)$ be the graph of the function f. The question is, how many *directions* can be *determined* by the graph of f. We have already seen Definition 0.13.

Definition 0.13 (Direction set)**.** If $\mathcal{U}$ denotes an arbitrary set of points in the affine plane $\mathrm{AG}(2,q)$ then we say that the set

$$\mathcal{D} = \left\{ \frac{b-d}{a-c} \;\middle|\; (a,b),(c,d) \in \mathcal{U}, (a,b) \neq (c,d) \right\}$$

is the *set of directions determined by* $\mathcal{U}$. We define $\frac{a}{0}$ as ∞ if $a \neq 0$, thus $\mathcal{D} \subseteq \mathrm{GF}(q) \cup \{\infty\}$. If $\mathcal{U}$ is the graph of a function, then it simply means that $|\mathcal{U}| = q$ and $\infty \notin \mathcal{D}$.

We mention here the structure theorem 0.16 of Blokhuis, Ball, Brouwer, Storme and Szőnyi ([15], [11]). To recall their result we need some definitions.

Definition 2.1. Let $\mathcal{U}$ be a set of points of $\mathrm{AG}(2,q)$, $q = p^h$. If $y \in \ell_\infty$ is an arbitrary direction, then let $s(y)$ denote the greatest power of p such that each line ℓ of direction y meets $\mathcal{U}$ in zero modulo $s(y)$ points. In other words,

$$s(y) = \gcd\left(\left\{|\ell \cap \mathcal{U}| \;\middle|\; \ell \cap \ell_\infty = \{y\}\right\} \cup \{p^h\}\right).$$

Let s be the greatest power of p such that each line ℓ of direction in $\mathcal{D}$ meets $\mathcal{U}$ in zero modulo s points. In other words,

$$s = \gcd_{y \in \mathcal{D}} s(y) = \min_{y \in \mathcal{D}} s(y).$$

Note that $s(y)$ and thus also s might be equal to 1. Note that $s(y) = 1$ for each non-determined direction $y \notin \mathcal{D}$.

Remark 2.2. Suppose that $s \geq p$. Then for each line $\ell \subset \mathrm{PG}(2,q)$:

either	$(\mathcal{U} \cup \mathcal{D}) \cap \ell = \emptyset$;
or	$\lvert(\mathcal{U} \cup \mathcal{D}) \cap \ell\rvert \equiv 1 \pmod{s}$.

Moreover, $|\mathcal{U}| \equiv 0 \pmod{s}$.

(If $s = 1$ then $0 \equiv 1 \pmod{s}$.)

Proof. Fix a direction $y \in \mathcal{D}$. Each affine line with slope y meets $\mathcal{U}$ in zero modulo s points, so $|\mathcal{U}| \equiv 0 \pmod{s}$.
An affine line $L \subset \mathrm{AG}(2,q)$ with slope $y \in \mathcal{D}$ meets $\mathcal{U}$ in $0 \pmod{s}$ points, so the *projective* line $\ell = L \cup \{y\}$ meets $\mathcal{U} \cup \mathcal{D}$ in $1 \pmod{s}$ points.
An affine line $L \subset \mathrm{AG}(2,q)$ with slope $y \notin \mathcal{D}$ meets $\mathcal{U}$ in at most one point, so the *projective* line $\ell = L \cup \{y\}$ meets $\mathcal{U} \cup \mathcal{D}$ in either zero or one point.
Let $P \in \mathcal{U}$ and let $L \subset \mathrm{AG}(2,q)$ an affine line with slope $y \in \mathcal{D}$, such that $P \in L$. Then the *projective* line $\ell = L \cup \{y\}$ meets $\mathcal{U}$ in $0 \pmod{s}$ points, and thus, ℓ meets $\mathcal{D} \cup \mathcal{U} \setminus \{P\}$ also in $0 \pmod{s}$ points. Thus, considering all the lines through P (with slope in $\mathcal{D}$), we get $|\mathcal{U} \cup \mathcal{D}| \equiv 1 \pmod{s}$. Since $\mathcal{U}$ has $0 \pmod{s}$ points, $|\mathcal{D}| \equiv 1 \pmod{s}$. So we get that $\mathcal{U} \cup \mathcal{D}$ meets also the ideal line in $1 \pmod{s}$ points. □

Remark 2.3 (Blocking set of Rédei-type). If $|\mathcal{U}| = q$ then each of the q affine lines with slope $y \notin \mathcal{D}$ meets $\mathcal{U}$ in exactly one point, so $\mathcal{B} = \mathcal{U} \cup \mathcal{D}$ is a blocking set meeting each projective line in 1 (mod s) points. Moreover, if $\infty \notin \mathcal{D}$ then $\mathcal{U}$ is the graph of a function, and such a blocking set $\mathcal{B}$ above is called *of Rédei-type*.

Definition 2.4 (Affine linear set). A GF(s)-*linear affine set* is the GF(s)-linear span of some vectors in $\mathrm{AG}(n,q) \cong \mathrm{GF}(s^{\log_s q})^n \cong \mathrm{GF}(s)^{n \log_s q}$ (or possibly a translate of such a span). The *rank* of the affine linear set is the rank of this span over GF(s).

Now we can recall Theorem 0.16.

Theorem 0.16 (Blokhuis-Ball-Brouwer-Storme-Szőnyi, Ball, [15], [11]). *Let $|\mathcal{U}| = q$ and $\infty \notin \mathcal{D}$. Using the notation s defined above, one of the following holds:*

$$\begin{array}{llll} \textbf{either} & s = 1 & \textit{and} & \dfrac{q+3}{2} \le |\mathcal{D}| \le q; \\ \textbf{or} & \mathrm{GF}(s) \textit{ is a subfield of } \mathrm{GF}(q) & \textit{and} & \dfrac{q}{s} + 1 \le |\mathcal{D}| \le \dfrac{q-1}{s-1}; \\ \textbf{or} & s = q & \textit{and} & |\mathcal{D}| = 1. \end{array}$$

Moreover, if $s > 2$ then $\mathcal{U}$ is a GF(s)*-linear affine set (of rank* $\log_s q$*).* □

What about the directions determined by an affine set $\mathcal{U} \subseteq \mathrm{AG}(2,q)$ of cardinality *not* q? Remember that if $|\mathcal{U}| > q$ then it determines all the $q+1$ directions. So we can restrict our research to affine sets of *less than* q points.

Examining the case $q = p$ prime, we mention Theorem 0.17 proved by Szőnyi [50] and later (independently) also by Blokhuis, which is an extension of the Rédei-Megyesi theorem 0.14.

Theorem 0.17 (Szőnyi, [50]). *Let $q = p$ prime and suppose that $1 < |\mathcal{U}| \le p$. Also suppose that $\infty \notin \mathcal{D}$. Then*

$$\begin{array}{lll} \textbf{either} & \dfrac{|\mathcal{U}|+3}{2} \le |\mathcal{D}| \le p; \\ \textbf{or} \quad \mathcal{U} \textit{ is collinear} & \textit{and} & |\mathcal{D}| = 1. \end{array}$$

Moreover, these bounds are sharp. □

In this chapter our aim is to generalize this result to the $q = p^h$ prime *power* case by proving an analogue of Theorem 0.16 for the case $|\mathcal{U}| \le q$.

2.2 The Rédei polynomial of less than q points

Here we describe the process as it is a nice illustration of the use of the polynomial method in the direction problem. Let $\mathcal{U}$ be a set of less than q affine points in $\mathrm{AG}(2,q)$, and let $n = |\mathcal{U}|$. Here we use the following form of the Rédei-polynomial: let $R(X,Y)$ inhomogeneous polynomial of the affine set $\mathcal{U}$, that is,

$$R(X,Y) = \prod_{(a,b)\in\mathcal{U}} (X - aY + b) = X^n + \sum_{i=0}^{n-1} \sigma_{n-i}(Y)X^i$$

where the abbreviation $\sigma_k(Y)$ means the k-th elementary symmetric polynomial of the set $\{b - aY \mid (a,b) \in \mathcal{U}\}$ of linear polynomials.

Proposition 2.5. *If $y \in \mathcal{D}$ then $R(X,y) \in \mathrm{GF}(q)[X^{s(y)}] \setminus \mathrm{GF}(q)[X^{p\cdot s(y)}]$.*
If $y \notin \mathcal{D}$ then $R(X,y) \mid X^q - X$.

Proof. Assume $y \in \mathcal{D}$. Then the equation $R(X,y) = 0$ has root x with multiplicity m if there is a line with slope y meeting $\mathcal{U}$ in exactly m points. The value of x determines this line. So each x is either not a root of $R(X,y)$ or a root with multiplicity a multiple of $s(y)$; and $p \cdot s(y)$ does not have this property. Since R is totally reducible, it is the product of its root factors.
If $y \notin \mathcal{D}$ then a line with direction y cannot meet $\mathcal{U}$ in more than one point, so an x cannot be a multiple root of $R(X,y)$. □

Notation. Let $\mathbb{F}$ be the polynomial ring $\mathrm{GF}(q)[Y]$ and consider $R(X,Y)$ as the element of the univariate polynomial ring $\mathbb{F}[X]$. Divide $X^q - X$ by $R(X,Y)$ as a univariate polynomial over $\mathbb{F}$ and let Q denote the quotient and let $H + X$ be the negative of the remainder.

$$\begin{aligned} Q(X,Y) &= (X^q - X) \quad \text{div } R(X,Y) && \text{over} \quad \mathbb{F} \\ -X - H(X,Y) &\equiv (X^q - X) \quad \text{mod } R(X,Y) && \text{over} \quad \mathbb{F} \end{aligned}$$

So

$$R(X,Y)Q(X,Y) = X^q + H(X,Y) = X^q + \sum_{i=0}^{q-1} h_{q-i}(Y)X^i$$

where $\deg_X H < \deg_X R$. Let σ^* denote the coefficients of Q,

$$Q(X,Y) = X^{q-n} + \sum_{i=0}^{q-n-1} \sigma^*_{q-n-i}(Y)X^i$$

and so

$$h_j(Y) = \sum_{i=0}^{j} \sigma_i(Y)\sigma^*_{j-i}(Y).$$

We know that $\deg h_i \leq i$, $\deg \sigma_i \leq i$ and $\deg \sigma_i^* \leq i$. Note that the $\sigma^*(Y)$ polynomials are not necessarily elementary symmetric polynomials of linear polynomials and if $y \in \mathcal{D}$ then $Q(X, y)$ is not necessarily totally reducible.

Remark 2.6. Since $\deg_X H < \deg_X R$, we have $h_i = 0$ for $1 \leq i \leq q - n$. By definition, $\sigma_0 = \sigma_0^* = 1$. The equation $h_1 = 0$ implies $\sigma_1^* = -\sigma_1$, this fact and the equation $h_2 = 0$ implies $\sigma_2^* = -\sigma_2 + \sigma_1^2$ and so on, the $q-n$ equations $h_i = 0$ uniquely define all the coefficients σ_i^*.

Proposition 2.7. *If $y \in \mathcal{D}$ then $Q(X, y), H(X, y) \in \mathrm{GF}(q)[X^{s(y)}]$ and if $\deg R \leq \deg Q$ then $Q(X, y) \in \mathrm{GF}(q)[X^{s(y)}] \setminus \mathrm{GF}(q)[X^{p \cdot s(y)}]$.*
If $y \notin \mathcal{D}$ then $R(X, y)Q(X, y) = X^q + H(X, y) = X^q - X$. In this case $Q(X, y)$ is also a totally reducible polynomial. □

Remark 2.8. Note that $H(X, y)$ can be an element of $\mathrm{GF}(q)[X^{p \cdot s(y)}]$. If $H(X, y) \equiv a$ is a constant polynomial, then $R(X, y)Q(X, y) = X^q + a = X^q + a^q = (X + a)^q$. This means that $R(X, y) = (X + a)^n$ and thus, there exists exactly one line (corresponding to $X = -a$) of direction y that contains $\mathcal{U}$, and so $\mathcal{D} = \{y\}$.

The following definition will be essential in order to state our main result.

Definition 2.9. If $|\mathcal{D}| \geq 2$ (i.e. $H(X, y)$ is not a constant polynomial) then for each $y \in \mathcal{D}$, let $t(y)$ denote the maximal power of p such that $H(X, y) = f_y(X)^{t(y)}$ for some $f_y(X) \notin \mathrm{GF}(q)[X^p]$.

$$H(X, y) \in \mathrm{GF}(q)[X^{t(y)}] \setminus \mathrm{GF}(q)[X^{t(y)p}].$$

In this case $t(y) < q$ since $t(y) \leq \deg_X H < q$. Let t be the greatest common divisor of the numbers $t(y)$, that is,

$$t = \gcd_{y \in \mathcal{D}} t(y) = \min_{y \in \mathcal{D}} t(y).$$

If $H(X, y) \equiv a$ (i.e. $\mathcal{D} = \{y\}$) then we define $t = t(y) = q$.

Remark 2.10. If there exists at least one determined direction $y \in \mathcal{D}$ such that $H(X, y)$ is not constant then $t < q$. From Proposition 2.7 we have $s(y) \leq t(y)$ for all $y \in \mathcal{D}$, so $s \leq t$. □

Proposition 2.11. *Using the notation above,*

$$R(X, Y)Q(X, Y) = X^q + H(X, Y) \in \mathrm{Span}_{\mathbb{F}}\langle 1, X, X^t, X^{2t}, X^{3t}, \ldots, X^q \rangle.$$

□

2.3 Bounds on the number of directions

Although, in the original problem, the vertical direction ∞ was not determined, from now on, without loss of generality we suppose that ∞ is a determined direction (if not, we apply an affine collineation). We continue to suppose that there is at least one non-determined direction.

We will use the following two remarks.

Lemma 2.12. *If $\infty \in \mathcal{D} \subsetneqq \ell_\infty$ then $|\mathcal{D}| \geq \deg_X H(X,Y) + 1$.* □

Lemma 2.13. *Let $\kappa(y)$ denote the number of the roots of $X^q + H(X,y)$ in $\mathrm{GF}(q)$, counted with multiplicity. If $X^q + H(X,y) \neq X^q - X$ and if $H(X,y)$ is not a constant polynomial, then*

$$\frac{\kappa(y)-1}{t(y)+1} + 1 = \frac{\kappa(y)+t(y)}{t(y)+1} \leq t(y) \cdot \deg f_y(X) = \deg_X H \leq \deg H.$$

□

Using these lemmata above we can prove a theorem similar to Theorem 0.16, and this is our main result here.

Theorem 2.14. *Let $\mathcal{U} \subset \mathrm{AG}(2,q)$ be an arbitrary set of points and let $\mathcal{D}$ denote the directions determined by $\mathcal{U}$. We use the notation s and t defined above geometrically and algebraically, respectively. Suppose that $\infty \in \mathcal{D}$. One of the following holds:*

either	$1 = s \leq t < q$	*and*	$\dfrac{\lvert\mathcal{U}\rvert - 1}{t+1} + 2 \leq \lvert\mathcal{D}\rvert \leq q+1;$
or	$1 < s \leq t < q$	*and*	$\dfrac{\lvert\mathcal{U}\rvert - 1}{t+1} + 2 \leq \lvert\mathcal{D}\rvert \leq \dfrac{\lvert\mathcal{U}\rvert - 1}{s-1};$
or	$1 \leq s \leq t = q$	*and*	$\mathcal{D} = \{\infty\}.$

Proof. The third case is trivial ($t = q$ means $|\mathcal{D}| = 1$, by the definition of t).
Let P be a point of $\mathcal{U}$ and consider the lines connecting P and the ideal points of $\mathcal{D}$. Since each such line meets $\mathcal{U}$ and has a direction determined by $\mathcal{U}$, it is incident with $\mathcal{U}$ in a multiple of s points. If $s > 1$ then counting the points of $\mathcal{U}$ on these lines we get the upper bound.
If $t < q$ then we can choose a direction $y \in \mathcal{D}$ such that the conditions of Lemma 2.13 hold. Using Lemma 2.12 and Lemma 2.13, we get

$$|\mathcal{D}| \geq \deg_X H(X,Y) + 1 \geq \frac{\kappa(y)-1}{t(y)+1} + 1 + 1.$$

The number of roots of $R(X,y)Q(X,y)$ is at least the number of roots of $R(X,y)$ which equals to $|\mathcal{U}|$. Thus $\kappa(y) \geq |\mathcal{U}|$. And thus

$$\frac{\kappa(y)-1}{t(y)+1} \geq \frac{|\mathcal{U}|-1}{t+1}.$$

□

An affine collineation converts Szőnyi's Theorem 0.17 to the special case of Theorem 2.14, since t is equal to either 1 or p in the case $q = p$ prime.

In the case $q > p$, the main problem of Theorem 2.14 is that the definition of t is non-geometrical. Unfortunately, $t = s$ does not hold in general. For example, let $\mathcal{U}$ be a $\mathrm{GF}(p)$-linear set minus one point. In this case $s = 1$, but $t = p$. In the rest of this chapter, we try to describe this problem.

2.4 Maximal affine sets

In this section we have the focus on point sets which are not extendable.

Definition 2.15 (Maximal affine set)**.** We say that $\mathcal{U} \subseteq \mathrm{AG}(2, q)$ is a *maximal* affine set that determines the set $\mathcal{D} \subseteq \ell_\infty \cong \mathrm{PG}(1, q)$ of directions if each affine set that contains $\mathcal{U}$ as a *proper* subset determines *more than* $|\mathcal{D}|$ directions.

Stability theorems (e. g. in [49], generalized in [47]) stimulate us to restrict ourselves to examine the *maximal* affine sets only.

If we examine polynomials in one variable instead of Rédei-polynomials, we can get similar stability results. Such polynomials occur when we examine $R(X, y)$, $Q(X, y)$ and $H(X, y)$, or R, Q and H over $\mathrm{GF}(q)(Y)$. One may think that if "almost all" roots of a polynomial $g \in \mathrm{GF}(q)[X]$ have multiplicity a power of p then the quotient $X^q \ \operatorname{div} g$ extends g to a polynomial in $\mathrm{GF}(q)[X^p]$. We can prove more.

Notation. Let $p = \mathrm{char}\mathbb{F} \neq 0$ be the characteristic of the *arbitrary* field $\mathbb{F}$. Let $s = p^e$ and $q = p^h$ two arbitrary powers of p such that $e \leq h$ (i.e. $s \mid q$ but q is not necessarily a power of s).

Theorem 2.16. *Let $g, f \in \mathbb{F}[X]$ be polynomials such that $g \cdot f \in \mathbb{F}[X^s]$. If $0 \leq \deg f \leq s-1$ then $X^q \ \operatorname{div} g$ extends g to a polynomial in $\mathbb{F}[X^s]$.* □

This theorem above suggests that if the product $R(X, y)Q(X, y)$ is an element of $\mathrm{GF}(q)[Y][X^{p \cdot s(y)}]$ while $R(X, y) \in \mathrm{GF}(q)[Y][X^{s(y)}] \setminus \mathrm{GF}(q)[Y][X^{p \cdot s(y)}]$, then an extendability result might be in the background. If $\mathcal{U}$ is a maximal affine set then it cannot be completed, so we conjecture the following.

Conjecture 2.17. *If $\mathcal{U}$ is a* maximal *affine set that determines the set $\mathcal{D}$ of directions then $t(y) = s(y)$ for all $y \in \mathcal{D}$ where $t(y) > 2$.*

Note that there exist maximal affine sets which are not linear.

Example 2.18 (Non-linear maximal affine set)**.** Let $\mathcal{U} \subset \mathrm{AG}(2,q)$ be a set, $|\mathcal{U}| = q$, $s = 1$, $q \geq |\mathcal{D}| \geq \dfrac{q+3}{2}$. In this case $\mathcal{U}$ cannot be linear because then s would be at least p. But $\mathcal{U}$ must be maximal since $q+1$ points in $\mathrm{AG}(2,q)$ would determine all directions. Embed $\mathrm{AG}(2,q)$ into $\mathrm{AG}(2,q^m)$ as a subgeometry. Then $\mathcal{U} \subset \mathrm{AG}(2,q^m)$ is a maximal non-linear affine set of less than q^m points.

But if $s > 2$, we conjecture that a maximal set is linear.

Conjecture 2.19. *If $\mathcal{U}$ is a* maximal *affine set that determines the set $\mathcal{D}$ of directions and $t = s > 2$ then $\mathcal{U}$ is an affine* $\mathrm{GF}(s)$*-linear set.*

Although we conjecture that the maximal affine sets with $s = t > 2$ are linear sets, the converse is not true.

Example 2.20 (Non-maximal affine linear set)**.** Let $\mathrm{AG}(2,s^i)$ be a canonical subgeometry of $\mathrm{AG}(2, q = s^{i \cdot j})$ and let $\mathcal{U}$ be an affine $\mathrm{GF}(s)$-linear set in the subgeometry $\mathrm{AG}(2,s^i)$ that contains more than s^i points. Then $\mathcal{U}$ determines the same direction set that is determined by the subgeometry $\mathrm{AG}(2,s^i)$.

Chapter 3

On the structure of the directions not determined by a large affine point set

3.1 Introduction

In this chapter - which is based on [4] - we ascend from the plane and examine point sets in the n-dimensional space $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $q = p^h$.

Notation.

- Let $D \subseteq H_\infty$ denote the set of directions determined by the point set U.
- Let $N = H_\infty \setminus D$ denote the set of non-determined directions.
- α will usually refer to a non-determined direction.

Remember that the maximum cardinality of a point set, which does not determine every direction (i.e. every point at infinity), is q^{n-1}. The extendability problem is the following. Given a point set $U \subset \mathrm{AG}(n,q)$ of size less than q^{n-1}, not determining all the directions, the question is whether we can add some points to U to reach a set U' of cardinality q^{n-1} such that the set of determined directions remains the same, i.e. the sets U and U' determine exactly the same directions.

Some results on extendability of affine point sets not determining a given set of directions are known. These usually contain restrictions on the size of the affine point set or on the size of the set of the determined directions. The strongest results are known in the planar case. We recall Theorem 0.18 from [49].

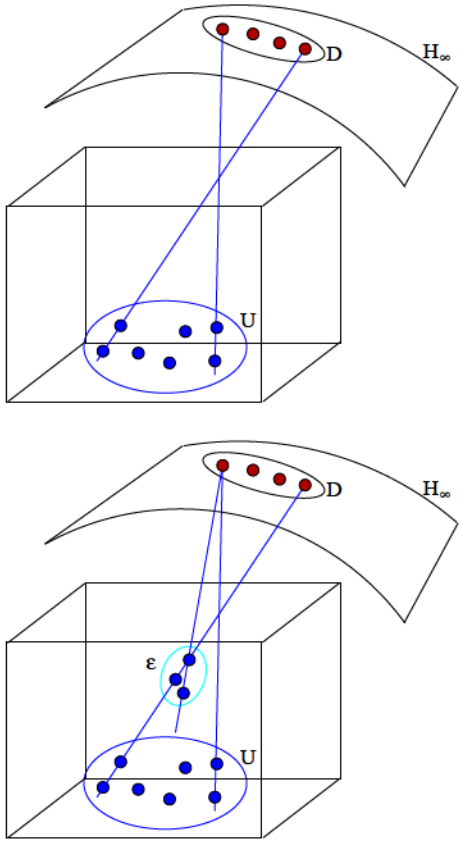

Figure 3.1: The extendability problem.

Theorem 0.18. *Let $U \subseteq \mathrm{AG}(2,q)$ be a set of affine points of size $q-\varepsilon > q-\sqrt{q}/2$, which does not determine a set N of more than $(q+1)/2$ directions. Then U can be extended to a set of size q, not determining the set N of directions.*

Theorem 0.20 is an extendability result for general dimension. Originally, it was proved in [22] for $n=3$. A proof for general n can be found in [12].

Theorem 0.20. *Let $q=p^h$, p an odd prime and $h>1$, and let $U \subseteq \mathrm{AG}(n,q)$, $n \geq 3$, be a set of affine points of size $q^{n-1}-2$, which does not determine a set N of at least $p+2$ directions. Then U can be extended to a set of size q, not determining the set N of directions.*

The natural question is whether Theorem 0.20 can be improved in the sense that extendability of sets of size $q^{n-1}-\varepsilon$ is investigated, for $\varepsilon > 2$, possibly with stronger assumptions on the number of non-determined directions.

In this chapter, we investigate affine point sets of size $q^{n-1}-\varepsilon$, for arbitrary ε, where the strongest results are obtained when ε is small. Instead of formulating an extendability result in terms of the *number* of non-determined directions, we formulate it in terms of the *structure* of the set of non-determined directions. To get the results, we use algebraic tools.

We give a detailed description of the polynomial method. We prove an extendability theorem for general dimensions if $|U| = q^{n-1} - 2$, and in 3 dimensions if $|U| = q^{n-1} - \varepsilon$, where $\varepsilon < p$. We will show that such a point set is typically extendable to a set of size q^{n-1}. If not, then the set N of non-determined directions has a strong structure, namely N is contained in an algebraic hypersurface of "low" degree. Finally, we add a section with applications of the obtained theorem.

3.2 The main result

Call up that we choose the coordinate system as follows. A point of $\mathrm{PG}(n,q)$ is represented by a homogenous $(n+1)$-tuple $(a_0, a_1, ..., a_n) \neq (0, 0, \ldots, 0)$. A hyperplane is the set of points whose coordinates satisfy a linear equation

$$a_0X_0 + a_1X_1 + \cdots + a_nX_n = 0$$

and so hyperplanes are represented by a homogenous $(n+1)$-tuple $[a_0, a_1, ..., a_n] \neq [0, 0, \ldots, 0]$. Embed the affine space $\mathrm{AG}(n,q)$ in $\mathrm{PG}(n,q)$ such that the hyperplane $X_0 = 0$, i.e. the hyperplane with coordinates $[1, 0, \ldots, 0]$ is the hyperplane at infinity of $\mathrm{AG}(n,q)$. Then the points of $\mathrm{AG}(n,q)$ will be coordinatized as $(1, a_1, a_2, ..., a_n)$.

The map δ from the points of $\mathrm{PG}(n,q)$ to its hyperplanes, mapping a point $(a_0, a_1, a_2, ..., a_n)$ to a hyperplane $[a_0, a_1, \ldots, a_n]$ is the standard duality of $\mathrm{PG}(n,q)$.

Let $U \subseteq \mathrm{AG}(n,q)$ be an affine point set, $|U| = q^{n-1} - \varepsilon$. Usually $\alpha = (0, \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n)$ refers to a point in H_∞ not determined by U.

Lemma 3.1. *Let $0 \leq r \leq n-2$. Let $\alpha = (0, \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n) \in N$ be a non-determined direction. Then each of the affine subspaces of dimension $r+1$ through α contain at most q^r points of U.*

Proof. We prove it by the pigeon hole principle. An affine subspace of dimension $r+1$ through α contains q^r affine (disjoint) lines through α, and each line contains at most one point of U as α is a non-determined direction. □

Definition 3.2. If an affine subspace of dimension $r+1 \leq n-1$ through $\alpha \in N$ contains less than q^r points of U, then it is called a *deficient subspace*. If it contains $q^r - t$ points of U, then its *deficiency* is t.

Corollary 3.3. *Let $T \subseteq H_\infty$ be a subspace of dimension $r \leq n-2$ containing $\alpha \in N$. Then there are precisely ε deficient subspaces of dimension $r+1$ (counted possibly with multiplicity) through T (a subspace with deficiency t is counted with multiplicity t).*

In particular:

Corollary 3.4. *There are precisely ε affine lines through $\alpha \in N$ not containing any point of U (and $q^{n-1}-\varepsilon$ lines with 1 point of U each).*

Now consider the set $U = \{(1, a_1^i, a_2^i, a_3^i, \ldots, a_n^i) : i = 1, ..., q^{n-1}-\varepsilon\}$. We write up its Rédei-polynomial as follows:

$$R(X_0, X_1, X_2, ..., X_n) = \prod_{i=1}^{q^{n-1}-\varepsilon} (X_0 + a_1^i X_1 + a_2^i X_2 + ... + a_n^i X_n).$$

Evoke that the intersection properties of the set U with hyperplanes of $\mathrm{PG}(n,q)$ are translated into algebraic properties of the polynomial R as follows. Consider $x_1, x_2, \ldots, x_n \in \mathrm{GF}(q)$, then $x \in \mathrm{GF}(q)$ is a root with multiplicity m of the equation $R(X_0, x_1, x_2, \ldots, x_n) = 0$ if and only if the hyperplane $[x, x_1, x_2, \ldots, x_n]$ contains m points of U.

Define the set $S(X_1, X_2, ..., X_n) = \{a_1^i X_1 + a_2^i X_2 + ... + a_n^i X_n : i = 1, ..., q^{n-1}-\varepsilon\}$, then R can be written as

$$R(X_0, X_1, X_2, ..., X_n) = \sum_{j=0}^{q^{n-1}-\varepsilon} \sigma_{q^{n-1}-\varepsilon-j}(X_1, X_2, ..., X_n) X_0^j,$$

where $\sigma_j(X_1, X_2, ..., X_n)$ is the j-th elementary symmetric polynomial of the set $S(X_1, X_2, ..., X_n)$.

Consider the subspace $s_{x_1,x_2,...,x_n} \subset H_\infty = [1, 0, ..., 0]$ of dimension $n-2$ which is the intersection of the hyperplanes $[x_0, x_1, x_2, ..., x_n]$, $x_0 \in \mathrm{GF}(q)$. Suppose that $s_{x_1,x_2,...,x_n}$ contains an undetermined direction. Then, by Lemma 3.1, each of the hyperplanes different from H_∞ through $s_{x_1,x_2,...,x_n}$ contains at most q^{n-2} points of U. This implies that there are precisely ε such hyperplanes (counted with multiplicity) through $s_{x_1,x_2,...,x_n}$ containing less than q^{n-2} points of U (a hyperplane with deficiency t is counted with multiplicity t). Algebraically, this means that for the $(n-2)$-dimensional subspace $s_{x_1,x_2,...,x_n}$,

$$R(X_0, x_1, x_2, ..., x_n) f(X_0) = (X_0^q - X_0)^{q^{n-2}} \tag{3.1}$$

where $f(X_0) = X_0^\varepsilon + \sum_{k=1}^{\varepsilon} f_k X_0^{\varepsilon-k}$ is a fully reducible polynomial of degree ε. Comparing the two sides of equation (3.1), one gets linear equations for the coefficients f_k of f in terms of the $\sigma_j(x_1, \ldots, x_n)$, and it is easy to see that the solution for each f_k is a polynomial expression in terms of the $\sigma_j(x_1, \ldots, x_n)$, $j = 1, \ldots, k$, use e.g. Cramer's rule to solve the system of equations, and notice that the determinant in the denominator equals 1. The polynomial expression is independent from the elements $x_1, x_2, \ldots, x_n$ (still under the assumption that $s_{x_1,x_2,...,x_n}$ does contain an undetermined direction), so we can change them for the variables $X_1, X_2, \ldots, X_n$ which makes the coefficients f_k polynomials in these variables; then the total degree of each $f_k(\sigma_j(X_1, \ldots, X_n) \ : \ j = 1, \ldots, n)$ is k.

Hence, using the polynomial expressions $f_k(\sigma_j : j)$, we can define the polynomial

$$f(X_0, X_1, \ldots, X_n) = X_0^\varepsilon + \sum_{k=1}^{\varepsilon} f_k(\sigma_1, \ldots, \sigma_k) X_0^{\varepsilon-k} \tag{3.2}$$

Clearly, $f(X_0, X_1, \ldots, X_n)$ is a polynomial of total degree ε, and, substituting $X_i = x_i$, $i = 1, \ldots, n$ for which $s_{x_1,\ldots,x_n}$ contains an undetermined direction, yields the polynomial $f(X_0, x_1, \ldots, x_n)$ that splits completely into ε linear factors. Also, since f contains the term X_0^ε, the point $(1, 0, 0, \ldots, 0)$ is not a root of f.

Suppose now that $f = \prod_i f_i$, where the polynomials $f_i(X_1, \ldots, X_n)$ are irreducible of degree ε_i, $\sum_i \varepsilon_i = \varepsilon$. Then each factor inherits the properties that (i) whenever the subspace $s_{x_1,x_2,\ldots,x_n} \subset H_\infty$ of dimension $n-2$ contains an undetermined direction, then $f_i(X_0, x_1, x_2, \ldots, x_n)$ splits into ε_i linear factors; and (ii) $(1, 0, \ldots, 0)$ is not a root of f_i. So from now on we will think of f as an irreducible polynomial satisfying (i) and (ii).

$f(X_0, X_1, \ldots, X_n) = 0$ is an algebraic hypersurface in the dual space $\mathrm{PG}(n, q)$. This consideration and the careful investigation of f using duality will be our key tool in order to reach the results. Our aim is to prove that the surface $f = 0$ splits into ε hyperplanes, or (equivalently) that it contains a linear factor (i.e. a hyperplane; then we can decrease ε by one, etc.). Therefore, we state and prove a series of technical lemmata.

Lemma 3.5. *Let $T \neq H_\infty$ be a deficient hyperplane through $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in N$ (i.e. T contains less than q^{n-2} points of U). Then in the dual space $\mathrm{PG}(n, q)$, T corresponds to an intersection point t of f and the hyperplane $[\alpha_0, \alpha_1, \ldots, \alpha_n]$.*

Proof. If $T = [x_0, x_1, \ldots, x_n]$ is a deficient hyperplane, then x_0 is a solution of the equation $f(X_0, x_1, x_2, \ldots, x_n) = 0$, hence, in the dual space $\mathrm{PG}(n, q)$, $t = (x_0, x_1, \ldots, x_n)$ is a point of the hypersurface defined by $f = 0$. If the hyperplane T contains the point $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in N$, then in the dual space the point t is contained in the hyperplane $[\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n]$. □

Lemma 3.6. *Let $(\alpha) \in N$ be a non-determined direction. Then in the dual space $\mathrm{PG}(n, q)$ the intersection of the hyperplane $[\alpha]$ and f is precisely the union of ε different subspaces of dimension $n-2$.*

Proof. First notice that

> If $(0, \alpha_1, \alpha_2, \ldots, \alpha_n) \in H_\infty = [1, 0, \ldots, 0]$ is an undetermined direction, then for all the subspaces $s_{x_1,x_2,\ldots,x_n} \subset H_\infty$ of dimension $n-2$ through $(0, \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$ the polynomial $f(X_0, x_1, x_2, \ldots, x_n)$ has precisely ε roots, counted with multiplicity.

translates to

> In the hyperplane $[0, \alpha_1, \alpha_2, ..., \alpha_n] \ni (1, 0, ..., 0)$, all the lines through $(1, 0, ..., 0)$ intersect the surface $f(X_0, x_1, x_2, ..., x_n) = 0$ in precisely ε points, counted with intersection multiplicity.

Define $\bar{f}$ as the surface of degree $\bar{\varepsilon} \leq \varepsilon$, which is the intersection of f and the hyperplane $[0, \alpha_1, \alpha_2, ..., \alpha_n]$. We know that all the lines through $(1, 0, ..., 0)$ intersect $\bar{f}$ in precisely ε points (counted with intersection multiplicity). So if $\bar{f} = \prod_i \bar{f}_i$, where $\bar{f}_i$ is irreducible of degree $\bar{\varepsilon}_i$ and $\sum_i \bar{\varepsilon}_i = \bar{\varepsilon}$, then we have that all the lines through $(1, 0, ..., 0)$ intersect $\bar{f}_i$ in precisely $\bar{\varepsilon}_i$ points (counted with intersection multiplicity).

By Corollary 3.4 we know that there are precisely ε different affine lines through the non-determined direction (α) not containing any point of U. In the dual space $\mathrm{PG}(n, q)$ these lines correspond to ε different subspaces of dimension $n - 2$ contained in the hyperplane $[\alpha]$. The deficient hyperplanes through these ε original lines correspond to the points of the subspaces in the dual. Hence by Lemma 3.5, all points of these subspaces are in f, which means that in $[\alpha]$ there are ε different subspaces of dimension $n - 2$ totally contained in f. □

Now we prove a lemma, which is interesting for its own sake as well.

Lemma 3.7. *Let $f(X_0, ..., X_n)$ be a homogeneous polynomial of degree $d < q$. Suppose that there are $n - 1$ independent concurrent lines $\ell_1, ..., \ell_{n-1}$ through the point P in $\mathrm{PG}(n, q)$ totally contained in the hypersurface $f = 0$. Then the hyperplane spanned by $\ell_1, ..., \ell_{n-1}$ is a tangent hyperplane of f.*

Proof. Without loss of generality, let $P = (1, 0, 0, ..., 0)$ and ℓ_i be the "axis":
$\ell_i = \langle P, \overset{0}{(1}, \overset{1}{0}, 0, ..., 0, \overset{i}{1}, 0, ..., \overset{n}{0})\rangle$, $i = 1, ..., n - 1$.
We want to prove that the hyperplane $x_n = 0$, i.e. $[0, ..., 0, 1]$ is tangent to f at P.

Firstly, observe that $\partial_{X_0} f(P) = 0$ as f has no term of type X_0^d since $f(P) = 0$.

Now we prove that $\partial_{X_i} f(P) = 0$ for all $i = 1, ..., n - 1$. As f vanishes on ℓ_i we have $f(sX_i, 0, ..., 0, X_i, 0, ..., 0) = 0$ for all substitutions to s and X_i. As $f(sX_i, 0, ..., 0, X_i, 0, ..., 0) = X_i^d f_0(s)$ for some f_0 with $\deg f_0 \leq d < q$, we have $f_0 \equiv 0$. In particular, f_0 has no term of degree $d - 1$, so f has no term of type $X_0^{d-1} X_i$. Hence $\partial_{X_i} f(1, 0, 0, ..., 0) = 0$. □

Corollary 3.8. *Let $f(X_0, ..., X_n)$ be a homogeneous polynomial of degree $d < q$. Suppose that in $\mathrm{PG}(n, q)$ the intersection of a hyperplane H and the hypersurface $f = 0$ contains two complete subspaces of dimension $n - 2$. Then H is a tangent hyperplane of f.*

Proof. Choose a point P in the intersection of the two subspaces of dimension $n-2$, the lines $\ell_1, ..., \ell_{n-2}$ through P in one of the subspaces and ℓ_{n-1} through P in the other such that $\ell_1, ..., \ell_{n-1}$ be independent and apply Lemma 3.7. □

Corollary 3.9. *If* $(\alpha) = (0, \alpha_1, \alpha_2, ..., \alpha_n) \in N \subset H_\infty$ *is a non-determined direction, then in the dual space* $\mathrm{PG}(n,q)$ *the hyperplane* $[\alpha]$ *is a tangent hyperplane of* f*. Note that* $[\alpha]$ *contains* $(1, 0, ..., 0)$*.*

Proof. By Lemma 3.6, the intersection of the hyperplane $[\alpha]$ and f is the union of ε different subspaces of dimension $n-2$. Then we can apply Corollary 3.8. □

Now we generalize Theorem 0.20.

Theorem 3.10. *Let* $n \geq 3$*. Let* $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$*,* $|U| = q^{n-1} - 2$*. Let* $D \subseteq H_\infty$ *be the set of directions determined by* U *and put* $N = H_\infty \setminus D$ *the set of non-determined directions. Then* U *can be extended to a set* $\bar{U} \supseteq U$*,* $|\bar{U}| = q^{n-1}$ *determining the same directions only, or the points of* N *are collinear and* $|N| \leq \lfloor \frac{q+3}{2} \rfloor$*, or the points of* N *are on a (planar) conic curve.*

Proof. Let $n \geq 3$. The hypersurface $f = 0$ is a quadric in the projective space $\mathrm{PG}(n,q)$. We will investigate the hyperplanes through the point $(1, 0, \ldots, 0)$ that meet $f = 0$ in exactly two $(n-2)$-dimensional subspaces. If the quadric $f = 0$ contains $(n-2)$-dimensional subspaces, then either $n = 3$ and the quadric is hyperbolic, or the quadric must be singular, since $\lfloor (n-1)/2 \rfloor$ is an upper bound for the dimension of the generators (i.e. the subspaces of maximum dimension contained in the quadric). If $f = 0$ contains 2 hyperplanes, then $f = 0$ is the product of two linear factors, counted with multiplicity. But then, by our remark before Lemma 3.5, the set U can be extended. Hence, if we suppose that the set U cannot be extended, the quadric $f = 0$ contains $(n-2)$-dimensional subspaces. Hence $f = 0$ is a cone such that its vertex is an $(n-3)$-dimensional subspace and the base is a (planar) conic, or it is a cone such that the vertex is an $(n-4)$-dimensional subspace and the base is a hyperbolic quadric in a 3-space. (Note that the second one contains the case when $n = 3$ and f is a hyperbolic quadric itself.) Denote in both cases the vertex by V.

Firstly suppose that $f = 0$ has an $(n-3)$-dimensional subspace V as vertex. A hyperplane $[\alpha]$ through $(1, 0, \ldots, 0)$ that meets the quadric $f = 0$ in exactly two $(n-2)$-dimensional subspaces must contain V and meets the base conic in two points (counted with multiplicity). Hence $[\alpha]$ is one of the $(q+1)$ hyperplanes through the span of $\langle (1, 0, \ldots, 0),\ V \rangle$. Dually, the undetermined direction (α) is a point of the line, which is the intersection of the dual (plane) of V and H_∞. When q is odd, there are $\frac{q+1}{2}$, respectively $\frac{q+3}{2}$ such hyperplanes meeting the base conic, depending on whether the vertex V is projected from the point $(1, 0, \ldots, 0)$ onto

an internal point, respectively, an external point of the base conic. When q is even, there are $\frac{q}{2}$ such hyperplanes.

Secondly suppose that $f = 0$ has an $(n-4)$-dimensional subspace V as vertex. Now a hyperplane $[\alpha]$ through $(1, 0, \ldots, 0)$ contains V and it meets the base quadric in two lines, i.e. a tangent plane to this hyperbolic quadric. Hence $[\alpha]$ is one of the q^2+q+1 hyperplanes through the span of $\langle (1, 0, \ldots, 0),\ V \rangle$. Dually, the undetermined direction (α) is a point of the plane, which is the intersection of the dual (3-space) of V and H_∞.

Among these hyperplanes only those count which meet the base hyperbolic quadric in two lines, i.e. those which intersect the base 3-space in such a tangent plane of the hyperbolic quadric, which goes through the projection of V from the point $(1, 0, \ldots, 0)$. Dually these hyperplanes form a conic, so (α) is a point of this conic. □

We consider the case when U is extendable as the typical one: otherwise, as we have seen, N has a very restricted (strong) structure; although note that there exist examples of maximal point sets U, of size $q^2 - 2$, $q \in \{3, 5, 7, 11\}$, not determining the points of a conic at infinity. These examples occur in the theory of maximal partial ovoids of generalized quadrangles, and were studied in [27], [19], and [21]. Non-existence of such examples for $q = p^h$, p an odd prime, $h > 1$, was shown in [22].

Now we prove a general extendability theorem in the 3-space if $\varepsilon < p$.

Theorem 3.11. *Let $U \subset \mathrm{AG}(3, q) \subset \mathrm{PG}(3, q)$, $|U| = q^2 - \varepsilon$, where $\varepsilon < p$. Let $D \subseteq H_\infty$ be the set of directions determined by U and put $N = H_\infty \setminus D$ the set of non-determined directions. Then N is contained in a plane curve of degree $\varepsilon^4 - 2\varepsilon^3 + \varepsilon$ or U can be extended to a set $\bar{U} \supseteq U$, $|\bar{U}| = q^2$.*

Proof. We proceed as before: we define the Rédei-polynomial of U, then we calculate $f(X_0, X_1, X_2, X_3)$ of degree ε. Suppose that U is not extendable; we investigate the structure of set N, the non-determined directions.

Finally we realize that for each triple (α, β, γ), if $(0, \alpha, \beta, \gamma) \in N \subset H_\infty$ is an undetermined direction then in the dual space $\mathrm{PG}(3, q)$ the plane $[0, \alpha, \beta, \gamma]$, which apparently goes through the point $(1, 0, 0, 0)$, is a tangent plane of the surface $f = 0$.

The tangent planes of f are of the form

$$[\partial_{X_0} f(a, b, c, d), \partial_{X_1} f(a, b, c, d), \partial_{X_2} f(a, b, c, d), \partial_{X_3} f(a, b, c, d)]$$

where (a, b, c, d) is a smooth point of f, and there are some others going through points of f where $\partial_{X_0} f = \partial_{X_1} f = \partial_{X_2} f = \partial_{X_3} f = 0$. For planes of both type containing $(1, 0, 0, 0)$ we have $\partial_{X_0} f(a, b, c, d) = 0$, so we get that the triples (α, β, γ), with $(0, \alpha, \beta, \gamma) \in H_\infty$ being an undetermined direction, correspond in the dual space $\mathrm{PG}(3, q)$ to tangent planes $[0, \alpha, \beta, \gamma]$

of $f = 0$ in points (a, b, c, d) which belong to the intersection of f and $\partial_{X_0} f$, which is a space curve $\mathcal{C}$ of degree $\varepsilon(\varepsilon - 1)$. Projecting these tangent planes from $(1, 0, 0, 0)$ (which all they contain) onto a (fixed) plane we get that in that plane the projected images $[\alpha, \beta, \gamma]$ are tangent lines of the projected image $\hat{\mathcal{C}}$, which is a plane curve of degree $\varepsilon(\varepsilon-1)$. So we get that the undetermined directions are contained in a plane curve of degree $\varepsilon(\varepsilon-1)\Big(\varepsilon(\varepsilon-1)-1\Big) = \varepsilon^4 - 2\varepsilon^3 + \varepsilon$. □

To reach the total strength of this theory, we would like to use an argument stating that it is a "very rare" situation that in $\mathrm{PG}(n, q)$ a hypersurface $f = 0$ with $d = \deg f > 2$ admits a hyperplane H such that the intersection of H and the hypersurface splits into d linear factors, i.e. $(n-2)$-dimensional subspaces. We will call such a hyperplane a TRI hyperplane, where the abbreviation TRI stands for Totally Reducible Intersection. We conjecture the following.

Conjecture 3.12. *Let $f(X_0, X_1, ..., X_n)$ be a homogeneous irreducible polynomial of degree $d > 2$ and let F be the hypersurface in $\mathrm{PG}(n, q)$ determined by $f = 0$. Then the number of TRI hyperplanes to F is "small" or F is a cone with a low dimensional base.*

By small we mean the existence of a function (upper bound) $r(d, n)$, which is independent from q; although we would not be surprised if even a constant upper bound, for instance $r(d, n) = 45$ would hold in general. By a low dimensional base of a cone we mean an at most 3-dimensional base.

We remark finally that such a result would immediately imply extendability of direction sets U under very general conditions.

3.3 An application

Here we describe an application of our stability theorem. We need the definition of *partial geometry*, introduced by Bose [18].

Definition 3.13. The incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is a (finite) *partial geometry*, if $\mathcal{P}$ and $\mathcal{B}$ are disjoint non-empty sets of objects called points and lines (respectively), and $\mathrm{I} \subseteq (\mathcal{P} \times \mathcal{B}) \cup (\mathcal{B} \times \mathcal{P})$ is a symmetric point-line incidence relation satisfying the following axioms:

(i) Each point is incident with $1 + t$ lines ($t \geqslant 1$) and two distinct points are incident with at most one line.

(ii) Each line is incident with $1 + s$ points ($s \geqslant 1$) and two distinct lines are incident with at most one point.

(iii) There exists a fixed integer $\alpha > 0$, such that if x is a point and L is a line not incident with x, then there are exactly α pairs $(y_i, M_i) \in \mathcal{P} \times \mathcal{B}$ for which x I M_i I y_i I L.

The integers s, t and α are the parameters of $\mathcal{S}$. The *dual* $\mathcal{S}^D$ of a partial geometry $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is the incidence structure $(\mathcal{B}, \mathcal{P}, \mathrm{I})$. It is a partial geometry with parameters $s^D = t$, $t^D = s$, $\alpha^D = \alpha$.

If $\mathcal{S}$ is a partial geometry with parameters s, t and α, then $|\mathcal{P}| = (s+1)\frac{(st+\alpha)}{\alpha}$ and $|\mathcal{B}| = (t+1)\frac{(st+\alpha)}{\alpha}$ (see e.g. [26]). A partial geometry with parameters s, t, and $\alpha = 1$ is a *generalized quadrangle* of order (s, t), [41]. We will use the abbreviation GQ.

To describe a class of partial geometries of our interest, we need some special point sets in $\mathrm{PG}(2, q)$. By Definition 0.6, an *arc of degree* d of a projective plane Π of order s is a set $\mathcal{K}$ of points such that every line of Π meets $\mathcal{K}$ in at most d points. If $\mathcal{K}$ contains k points, than it is also called a $\{k, d\}$-arc. The size of an arc of degree d can not exceed $ds - s + d$. A $\{k, d\}$-arc $\mathcal{K}$ for which $k = ds - s + d$, or equivalently, such that every line that meets $\mathcal{K}$, meets $\mathcal{K}$ in exactly d points, is called *maximal*. We call a $\{1, 1\}$-arc and a $\{s^2, s\}$-arc *trivial*. The latter is necessarily the set of s^2 points of Π not on a chosen line.

A typical example, in $\mathrm{PG}(2, q)$, is a conic, which is a $\{q+1, 2\}$-arc, which is not maximal, and it is well known that if q is even, a conic, together with its nucleus, is a $\{q+2, 2\}$-arc, which is maximal. We mention that a $\{q+1, 2\}$-arc in $\mathrm{PG}(2, q)$ is also called an *oval*, and a $\{q+2, 2\}$-arc in $\mathrm{PG}(2, q)$ is also called a *hyperoval*. When q is odd, all ovals are conics, and no $\{q+2, 2\}$-arcs exist ([44]). When q is even, every oval has a nucleus, and so can be extended to a hyperoval. Much more examples of hyperovals, different from a conic and its nucleus, are known, see e.g. [25]. We mention the following two general theorems on $\{k, d\}$-arcs.

Theorem 3.14 ([20]). *Let $\mathcal{K}$ be a $\{ds - s + d, d\}$-arc in a projective plane of order s. Then the set of lines external to $\mathcal{K}$ is a $\{s(s - d + 1)/d, s/d\}$-arc in the dual plane.*

As a consequence, $d \mid s$ is a necessary condition for the existence of maximal $\{k, d\}$-arcs in a projective plane of order s. The results for the Desarguesian plane $\mathrm{PG}(2, q)$ are much stronger. Denniston [28] showed that this condition is sufficient for the existence of maximal $\{k, d\}$-arcs in $\mathrm{PG}(2, q)$, q even. Blokhuis, Ball and Mazzocca [14] showed that non-trivial maximal $\{k, d\}$-arcs in $\mathrm{PG}(2, q)$ do not exist when q is odd. Hence, the existence of maximal arcs in $\mathrm{PG}(2, q)$ can be summarized in the following theorem.

Theorem 3.15. *Non-trivial maximal $\{k, d\}$-arcs in $\mathrm{PG}(2, q)$ exist if and only if q is even.*

Several infinite families and constructions of maximal $\{k, d\}$-arcs of $\mathrm{PG}(2, q)$, $q = 2^h$, and $d = 2^e$, $1 \leq e \leq h$, are known. We refer to [25] for an overview.

Let q be even and let $\mathcal{K}$ be a maximal $\{k,d\}$-arc of $\mathrm{PG}(2,q)$. We define the incidence structure $T_2^*(\mathcal{K})$ as follows. Embed $\mathrm{PG}(2,q)$ as a hyperplane H_∞ in $\mathrm{PG}(3,q)$. The points of $\mathcal{S}$ are the points of $\mathrm{PG}(3,q) \setminus H_\infty$. The lines of $\mathcal{S}$ are the lines of $\mathrm{PG}(3,q)$ not contained in H_∞, and meeting H_∞ in a point of $\mathcal{K}$. The incidence is the natural incidence of $\mathrm{PG}(3,q)$. One easily checks that $T_2^*(\mathcal{K})$ is a partial geometry with parameters $s = q-1$, $t = k-1 = (d-1)(q+1)$, and $\alpha = d-1$.

An *ovoid* of a partial geometry $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is a set $\mathcal{O}$ of points of $\mathcal{S}$, such that every line of $\mathcal{S}$ meets $\mathcal{O}$ in exactly one point. Necessarily, an ovoid contains $\frac{st}{\alpha}+1$ points. Different examples of partial geometries exist, and some of them have no ovoids, see e.g. [24]. The partial geometry $T_2^*(\mathcal{K})$ has always an ovoid. Consider any plane $\pi \neq H_\infty$ meeting H_∞ in a line skew to $\mathcal{K}$. The plane π then contains $\frac{st}{\alpha}+1 = q^2$ points of $\mathcal{S}$, and clearly every line of $\mathcal{S}$ meets π in exactly one point.

It is a natural stability question to investigate *extendability* of point sets of size slightly smaller than the size of an ovoid. In this case, the question is whether a set of points $\mathcal{B}$, with the property that every line meets $\mathcal{B}$ in at most one point, can be extended to an ovoid if $|\mathcal{B}| = q^2 - \varepsilon$, and ε is *not too big*. Such a point set $\mathcal{B}$ is called a *partial ovoid*, ε its *deficiency*, and it is called *maximal* if it cannot be extended. The following theorem is from [41] and deals with this question in general for GQs, i.e. for $\alpha = 1$.

Theorem 3.16 ([41]). *Consider a GQ of order (s,t). Any partial ovoid of size $(st-\rho)$, with $0 \leq \rho < t/s$ is contained in a uniquely defined ovoid.*

For some particular GQs, extendability beyond the given bound is known. For other GQs, no better bound is known, or examples of maximal partial ovoids reaching the upper bound, are known. For an overview, we refer to [23].

Let $\mathcal{H}$ be a hyperoval of $\mathrm{PG}(2,q)$. Consider the generalized quadrangle $T_2^*(\mathcal{H})$ defined as above. Theorem 3.16 yields that a partial ovoid of $T_2^*(\mathcal{H})$ of size q^2-2 can always be extended. The proof of Theorem 3.16 is of combinatorial nature, and can be generalized to study partial ovoids of partial geometries. However, for the partial geometries $T_2^*(\mathcal{K})$ with $\alpha \geq 2$, such an approach only yields extendability of partial ovoids with deficiency one. In the context of this chapter, we can study extendability of partial ovoids of the partial geometry $T_2^*(\mathcal{K})$ as a direction problem. Indeed, if a set of points $\mathcal{B}$ is a (partial) ovoid, then no two points of $\mathcal{B}$ determine a line of the partial geometry $T_2^*(\mathcal{K})$. Hence the projective line determined by two points of $\mathcal{B}$ must not contain a point of $\mathcal{K}$, in other words, the set of points $\mathcal{B}$ is a set of affine points, not determining the points of $\mathcal{K}$ at infinity.

Considering a partial ovoid $\mathcal{B}$ of size q^2-2, we can apply Theorem 3.10. Clearly, the non-determined directions, which contain the points of $\mathcal{K}$, do not satisfy the conditions when $\mathcal{B}$ is not extendable. Hence, we immediately have the following corollary.

Corollary 3.17. *Let $\mathcal{B}$ be a partial ovoid of size $q^2 - 2$ of the partial geometry $T_2^*(\mathcal{K})$, then $\mathcal{B}$ is always extendable to an ovoid.*

This result is the same as Theorem 3.16 for the GQ $T_2^*(\mathcal{H})$, $\mathcal{H}$ a hyperoval of PG$(2, q)$, $q > 2$.

Chapter 4

An extension of the direction problem

4.1 Introduction

In this chapter - which is based on [2] - we discuss a natural extension of the classical direction problem. First we describe the main concept of the recent generalization and give a summary of the definition and the results.

Notation.

- Capital letters denote subspaces, and the index of the letter refers to the dimension; e.g. S_k denotes a subspace of dimension k.

Originally, a point d at infinity (i.e. a direction) was said to be determined by a point set, if there were at least 2 points contained in the set lying on a line which had direction d. In other words, there is a 1-dimensional subspace with ideal point d spanned by 2 points of the set. Now we consider affine point sets in the n-dimensional projective space, and examine subspaces of the ideal hyperplane H_∞.

First, we extend the definition of *determined direction* in the following way:

Definition 4.1. Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$ be a point set, and k be a fixed integer, $k \leq n-2$. We say a *subspace* S_k of dimension k in H_∞ is *determined* by U if there is an affine subspace T_{k+1} of dimension $k+1$, having S_k as its hyperplane at infinity, containing at least $k+2$ affinely independent points of U (i.e. spanning T_{k+1}).

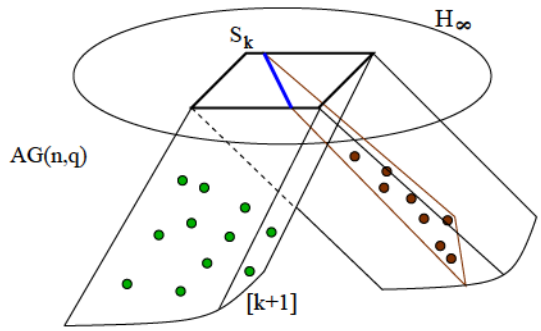

Figure 4.1: Points refer to the points of the set U. They span the left $(k+1)$-subspace, i. e. determine S_k; while the points in the right $(k+1)$-subspace would not determine S_k as they are not affinely independent.

The questions here also arose from the classical problem. That is, for a given point set U and for a fixed k how many subspaces of dimension k are determined by U and what can we say about the point set if there exist non-determined k-subspaces. Our aim is to describe the size and the structure of U, if it does not determine all the k-subspaces in H_∞. Note that in that case $|U| \leq q^{n-1}$ holds. (We will give the short proof of this easy fact in the next section.) It means that the maximal "interesting" point sets are of size q^{n-1}, and recall that this is the same as in the classical direction problem. Now we examine the extremal case, i. e. we are interested in point sets of size q^{n-1} not determining every k-subspace. In Section 4.2 we give a construction of such a point set, and we also describe a hierarchy of determined subspaces of different dimensions at H_∞. Section 4.3 is dedicated to the complete description of the case $n = 3$. We completely characterize the point sets of cardinality q^2. It will turn out that in 3 dimensions hyperbolic quadrics somehow play a main role among the point sets which do not determine many subspaces at infinity. In Section 4.4 we continue to examine quadrics in higher dimensions.

Differently from the previous chapters, instead of using strong algebraic tools, here we make purely geometrical and combinatorial considerations throughout the proofs.

4.2 The extremal case

Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$ be an affine point set. Consider a subspace S_k of dimension k at infinity. There are q^{n-k-1} (pairwise disjoint) affine subspaces of dimension $k+1$ with the ideal hyperplane S_k. Suppose that S_k is not determined, and consider an affine $(k+1)$-subspace T_{k+1} through S_k. Then the points of $U \cap T_{k+1}$ are contained in some subspace of dimension k since S_k is undetermined, hence T_{k+1} is not spanned by the points of U. An affine subspace of dimension k consists of q^k points, so (any) T_{k+1} can contain at most q^k

points of U. This implies $|U| \leq q^{n-1}$ if it does not determine all the k-subspaces at infinity.

We will examine point sets of the maximal interesting cardinality, so from now on let $|U| = q^{n-1}$ throughout the whole chapter. Our aim is to find out the structure of U, if there are relatively many undetermined subspaces at infinity.

Let $|U| = q^{n-1}$. Suppose that there exists an undetermined k-subspace $S_k \subset H_\infty$. Then in each of the q^{n-k-1} affine $(k+1)$-subspaces whose ideal hyperplane is S_k there lie exactly q^k points of U constituting one complete k-subspace.

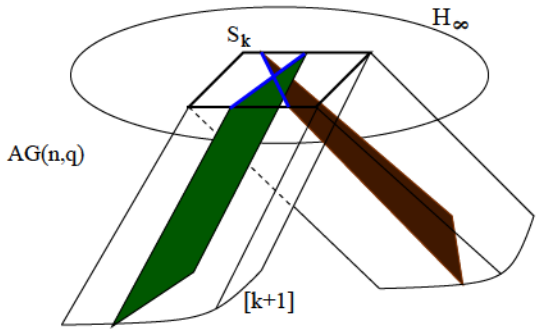

Figure 4.2: Non-determined k-subspace in the extremal case.

We can construct point sets not determining many subspaces in the following way:
Let $U_0 \subset \mathrm{AG}(m,q) \subset \mathrm{PG}(m,q)$, $|U_0| = q^{m-1}$. Denote by N_l^0 the set of the l-subspaces in H_∞ which are not determined by U_0. We can embed U_0 into $\mathrm{AG}(n,q)$, where $n > m$. Consider a subspace V on the ideal hyperplane of $\mathrm{AG}(n,q)$, $\dim V = v$, where $v = n-m-1$, completely disjoint from the original m-dimensional space. We construct a cone (cylinder) with base U_0 and vertex V such that we take the union of the affine subspaces spanned by a point of U_0 and the subspace V. These subspaces are of dimension $n-m$, and in that way we get a point set U in $\mathrm{AG}(n,q)$, $|U| = q^{n-1}$.
We will show that there are "many" subspaces at infinity which are not determined by U, and we characterize them.

Denote by N_r the set of subspaces of dimension r on the ideal hyperplane which are not determined by U.

Proposition 4.2. *Let $U_0 \subset \mathrm{AG}(m,q) \subset \mathrm{PG}(m,q)$, $|U_0| = q^{m-1}$ embedded into $\mathrm{AG}(n,q)$, let $V \subseteq H_\infty$ be a subspace in $PG(n,q)$ completely disjoint from $\mathrm{PG}(m,q)$, $\dim V = n-m-1$, let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$ be the cone (cylinder) constructed as above with base U_0 and vertex V. Let $W \subseteq H_\infty$ in $\mathrm{PG}(n,q)$, $\dim W = r$. Then W is non-determined, i.e. $W \in N_r$ if and only if, after projecting W from V to the m-space, the projected image $W_0 = \mathrm{PG}(m,q) \cap \langle V, W \rangle$ is non-determined by U_0.*

Proof. For the proof let $s = \dim(W \cap V)$ and $r_0 = \dim W_0 = r - s - 1$. (Note that W and W_0 are contained in the hyperplane at infinity.) By projection we always mean projection from the center V (see below).

Suppose that W is non-determined. Let $L_0 \supset W_0$ be any of the affine (r_0+1)-dimensional subspaces in $\mathrm{PG}(m,q)$ through W_0, we have to prove that $L_0 \cap U_0$ is a complete affine r_0-space. Take any affine point P from the subspace $\langle V, L_0\rangle$, then define $L = \langle P, W\rangle$. Now L_0 is the projected image of L, i.e. $L_0 = \mathrm{PG}(m,q) \cap \langle V, L\rangle$. As $\dim L = r+1$ and W is non-determined, $A = L \cap U$ must be a complete affine r-space. Hence $L_0 \cap U_0$ is the projected image of it, i.e. a complete affine r_0-space. (We have used the fact that $\dim(\bar{A} \cap V) = s = \dim(W \cap V)$, where $\bar{A}$ is the projective closure of A. Indeed, if $\dim(\bar{A} \cap V)$ were larger then $\dim(L \cap U)$ would be larger accordingly.) Hence W_0 is non-determined.

On the other hand, suppose that W_0 is non-determined. Then for any $(r+1)$-dimensional affine subspace L through W, and for its projected image L_0, the intersection $L_0 \cap U_0$ is identical to the projected image of $L \cap U$. As $L_0 \cap U_0$ is a complete (r_0+1)-dimensional affine subspace through W_0, we have that $L \cap U$ must be $\langle V, L_0\rangle \cap L$, i.e. a complete r-dimensional affine subspace through W. □

For a given affine point set we can examine determined subspaces in H_∞ of different dimensions. We are trying to find out a hierarchy of them. In [45] the following theorem was proved in the classical case:

Result 4.3 (Storme-Sziklai, [45]). *Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ and let $D \subseteq H_\infty$ be the set of directions determined by U. Then D is the union of some complete $(n-2)$-dimensional subspaces of H_∞.* □

We find an analogous situation in case of determining higher dimensional subspaces. First we note the following fact.

Observation 4.4. *Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ and k be a fixed integer, $k \leq n-3$. If there is a subspace S_k of dimension k, $S_k \subset H_\infty$ determined by U, then there is a subspace S_{k+1} of dimension $k+1$ in H_∞, $S_k \subset S_{k+1}$, which is determined by U.*

Proof. Since S_k is determined by U, there exists an affine $(k+1)$-dimensional subspace A_{k+1} with the ideal hyperplane S_k which contains at least $k+2$ linearly independent points from U. There will be at least one $(k+2)$-dimensional affine subspace A_{k+2}, $A_{k+1} \subset A_{k+2}$ containing at least one more point P from U. As $P \in A_{k+2} \setminus A_{k+1}$, A_{k+2} contains at least $k+3$ linearly independent points from U, hence its ideal hyperplane (of dimension $(k+1)$) will be determined. □

Corollary 4.5. *Analogously to Result 4.3, through any determined k-subspace S_k, there exists a determined $(n-2)$-subspace.* □

Proposition 4.6. *Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ and k be a fixed integer, $k \leq n-3$. If there is a subspace V_{n-2} of dimension $n-2$, $V_{n-2} \subset H_\infty$ such that all of the k-dimensional subspaces of V_{n-2} are determined by U then V_{n-2} is determined by U as well.*

Proof. Suppose that there is a subspace V_{n-2} of dimension $n-2$, $V_{n-2} \subset H_\infty$ which is not determined by U. We will show that there is a subspace V_k, $\dim V_k = k$, $V_k \subset V_{n-2}$ which is not determined by U. Each of the q affine $(n-1)$-subspaces whose ideal hyperplane is V_{n-2} contains precisely a whole $(n-2)$-subspace from U. Such an $(n-2)$-subspace has an ideal hyperplane of dimension $n-3$ contained in V_{n-2}, so these $(n-3)$-subspaces cannot cover all the points of V_{n-2}. Consider an uncovered point P, and take a subspace $V_k \subset V_{n-2}$, $\dim V_k = k$ containing P. V_{n-2} and each of the affine subspaces of dimension $k+1$ with the ideal hyperplane V_k span a subspace of dimension $n-1$. Such an $(n-1)$-subspace contains precisely a whole $(n-2)$-subspace from U. The intersection of the $(n-2)$-subspace from U and the $(k+1)$-subspace is a subspace of dimension k (since this $(n-2)$-subspace cannot contain the $(k+1)$-subspace because $P \in V_k$.) So each of the $(k+1)$-spaces with the ideal hyperplane V_k contains precisely a whole k-space from U which means that V_k is not determined by U. □

4.3 The 3-dimensional case

We have already seen an example for a point set of maximal cardinality having relatively many undetermined subspaces at infinity. Now we ask for other constructions for U with many non-determined subspaces in H_∞, and, to be much more general, we try to find out the structure of the point set if there exist undetermined subspaces. The aim of this section is to characterize point sets of maximal size in the 3-dimensional projective space. As it will turn out, the typical situation is that such a point set determines all the subspaces. Point sets with two non-determined subspaces have a strong structure, moreover, in case of at least three undetermined subspaces, the only example is the construction of Theorem 4.2. Recall the definition and the basic facts of determined subspaces in the special case $n = 3$.

Let $U \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$ be a point set. We say a line $\ell \subset H_\infty$ is determined by U if there is an affine plane with the ideal line ℓ containing at least three points of U which are not collinear. Let $|U| = q^2$ (as this is the maximal interesting size in case of $n = 3$). Suppose that there exists an undetermined line ℓ. Then each of the q affine planes whose ideal line is ℓ contains precisely a complete line of U.

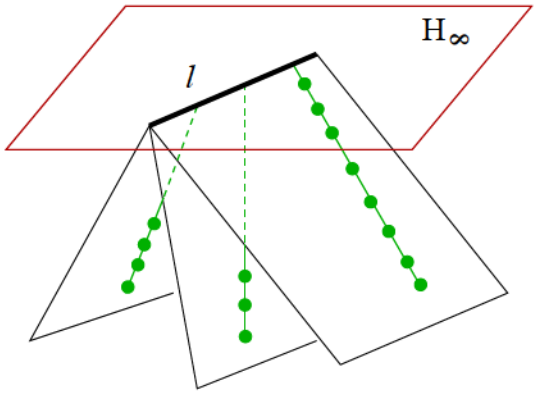

Figure 4.3: Non-determined line in the extremal case.

Our main result here is the complete characterization of point sets of maximal size. In the rest of this section we prove the following theorem:

Theorem 4.7. *Let $U \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$, $|U| = q^2$. Let L be the set of lines in H_∞ determined by U and put N the set of non-determined lines. Then one of the following holds:*

a) $|N| = 0$, *i.e. U determines all the lines of H_∞;*
b) $|N| = 1$ *and then there is a parallel class of affine planes such that U contains one (arbitrary) complete line in each of its planes;*
c) $|N| = 2$ *and then (i) U together with the two undetermined lines in H_∞ form a hyperbolic quadric or (ii) U contains q parallel lines (U is a cylinder);*
d) $|N| \geq 3$ *and then U contains q parallel lines (U is a cylinder).*

Proof. If all the points of U are contained in a plane, then U determines only one line, namely the ideal line of the plane containing U, so $|L| = 1$. It is a special case of **d)**.
So from now on suppose that U is not contained in a plane.
Denote by f_∞ the ideal point of an affine line f, and let $\bar{f} = f \cup f_\infty$.
$|N| = 0$ means that all the ideal lines are determined, so we cannot say anything about the structure of the point set (Case **a)**).
Case **b)** immediately follows from the remark before the theorem.
So from now on suppose that $|N| \geq 2$. Throughout this proof let $\ell_1, \ell_2 \subset H_\infty$ be undetermined lines, M the intersection point of ℓ_1 and ℓ_2.

Lemma 4.8. *Let f and g be affine lines contained in U, such that $\bar{f}$ intersects ℓ_1, $\bar{g}$ intersects ℓ_2. Then f and g meet each other or their ideal point is M.*

Proof of Lemma 4.8. Suppose to the contrary that $\bar{f}$ and $\bar{g}$ are skew lines, and at least for one of them, e. g. $\bar{f}$, $M \notin \bar{f}$. Then $\bar{f}$ intersects the plane s spanned by $\bar{g}$ and ℓ_2 at an affine point P not contained in g. Then P and g would determine ℓ_2, contradiction. ■

Lemma 4.9. *Consider the q affine lines contained in U whose ideal points are on ℓ_1. If there is a line f among them, such that $\bar{f}$ intersects ℓ_1 at M, then the ideal point of each of the q lines is M.*

Proof of Lemma 4.9. Suppose that there exists a line g contained in U, such that $\bar{g}$ intersects ℓ_1 not at M. Since $\bar{f}$ intersects ℓ_1 at M, it intersects ℓ_2 as well, so by Lemma 4.8 f meets g at an affine point P. Then the points of f and g would determine ℓ_1, contradiction. ■

Lemma 4.10. *If there exist f and g parallel affine lines contained in U, such that $\bar{f}$ and $\bar{g}$ intersect ℓ_1, then their ideal point is M.*

Proof of Lemma 4.10. Suppose to the contrary that $\bar{f}$ and $\bar{g}$ meet ℓ_1 not at M. Consider a point $P \in U$ not contained in the plane $\langle f, g \rangle$, and the plane s spanned by P and ℓ_2. (If $\nexists P \in U$ such that $P \notin \langle f, g \rangle$ then all the points of U would be contained in a plane.) s cannot be parallel to $\bar{f}$ and $\bar{g}$ as then they would intersect in the ideal hyperplane (i.e. on ℓ_2). So s intersects f and g at two different affine points. The two intersection points and P cannot be collinear as $P \notin \langle f, g \rangle$, so they would determine ℓ_2 as they span the plane s, contradiction. ■

Corollary 4.11. *If there exist f and g parallel affine lines contained in U, such that $\bar{f}$ and $\bar{g}$ intersect ℓ_1, then U consists of q parallel lines whose ideal point is M.*

Proof of Corollary 4.11. Since f and g are parallel, $\bar{f}$ and $\bar{g}$ meet at M due to Lemma 4.10. Then, by Lemma 4.9, for any line h contained in U whose ideal point is on ℓ_1, $\bar{h}$ will intersect ℓ_1 at M, which means that the q lines are all parallel. ■

Corollary 4.12. *If $|N| > 2$, $\ell_1 \subset H_\infty$ is an undetermined line, and there exist f, g parallel lines contained in U, such that $\bar{f}$ and $\bar{g}$ intersect ℓ_1, then all the undetermined lines in H_∞ has a common intersection point (and it is the ideal point of the lines of U).*

Proof of Corollary 4.12. Let ℓ_2, ℓ_3 be undetermined lines, M the intersection point of ℓ_1 and ℓ_2, K the intersection point of ℓ_1 and ℓ_3. By Lemma 4.10, $\bar{f}$ and $\bar{g}$ meet ℓ_1 at M and also at K. ■

Corollary 4.13. *If there exist 2 lines contained in U which are not parallel, and their ideal points are on ℓ_1, then all the q lines whose ideal points are on ℓ_1 have q different ideal points (and none of them is M).*

Proof of Corollary 4.13. Consider the q lines with ideal point on ℓ_1. By Corollary 4.11, if there exist two parallel lines among them, then all the q lines are parallel. Hence if they are not all parallel, then all of them are pairwise skew. It means that their ideal points on ℓ_1 are pairwise different. So there is a line $f \subset U$ such that $\bar{f}$ intersects ℓ_1 not at M. Then by Lemma 4.9 there cannot exist a line $g \subset U$ such that $\bar{g}$ intersects ℓ_1 at M. ■

So there are two different cases: **(1)** all the q lines meeting $\ell_1 \in N$ are parallel and intersect the ideal hyperplane at the intersection point of the undetermined lines or **(2)** all of them are pairwise skew.

In the first case U consists of q parallel lines (forming a cylinder). Without loss of generality we can assume that these are q vertical lines. The undetermined lines in H_∞ intersect each other at the ideal point of the vertical lines. Then every "horizontal" (affine) plane (intersecting the vertical lines) contains q points of U. Consider the directions not determined by these q points on a "horizontal" plane. The undetermined lines are exactly the lines connecting the ideal point of the vertical lines and an undetermined direction.
It is exactly the construction we saw in Proposition 4.2. The base of the cone is a point set of cardinality q contained in a horizontal plane, and the vertex of the cone is the point M. This gives the description of cases **c)** (ii) and **d)**.
There is a special case of this first case we have already seen right after the theorem: the q vertical lines can be co-planar. It means that U is contained in a plane. Then U determines only one line, so $|L| = 1$.

In the second case let ℓ_1, ℓ_2 be undetermined lines. By Corollary 4.13 we know that the points of U form q lines whose ideal points are on ℓ_1, and these ideal points are pairwise different, so the lines are skew. It also holds for ℓ_2, so U forms q skew lines whose ideal points are on ℓ_2, and these ideal points are pairwise different. Consider three of the skew lines whose ideal points are on ℓ_1 and denote them by f, g and h. By Lemma 4.8 all the q lines whose ideal points are on ℓ_2 intersect f, g and h at one-one point. The intersection points are different as the q lines are pairwise skew. So the q lines whose ideal points are on ℓ_2 form a q-regulus of f, g and h, and together with ℓ_1 it is a $(q+1)$-regulus of $\bar{f}$, $\bar{g}$ and $\bar{h}$. The same holds for the lines f', g' and h' whose ideal points are on ℓ_2: the q lines whose ideal points are on ℓ_1 together with ℓ_2 form a $(q+1)$-regulus of $\bar{f'}$, $\bar{g'}$ and $\bar{h'}$. It means that the q^2 points of U and the undetermined lines ℓ_1 and ℓ_2 form a hyperbolic quadric. This is Case **c)** (i) and so Theorem 4.7 is proved. □

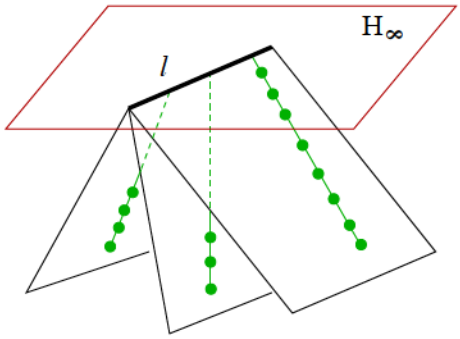

Figure 4.4: Theorem 4.7 b) $|N| = 1$ and U contains one (arbitrary) complete line in each plane of a parallel class of affine planes.

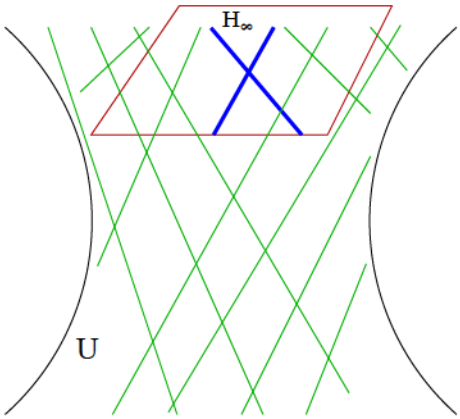

Figure 4.5: Theorem 4.7 c) $|N| = 2$ and U together with the two undetermined lines in H_∞ form a hyperbolic quadric.

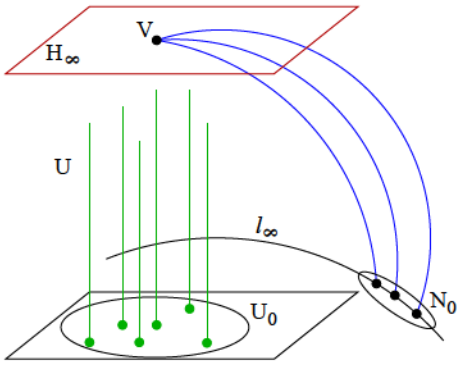

Figure 4.6: Theorem 4.7 d) $|N| \geq 3$ and U contains q parallel lines (U is a cylinder).

4.4 More quadrics

In the previous section we have seen the complete characterization of the sets of maximal cardinality in 3 dimensions. Our aim now is to find similar results in higher dimensions. In $\mathrm{PG}(n,q)$ we will show that if we try to find a point set U, $|U| = q^{n-1}$ which does not determine all the subspaces of a certain dimension then the former examples will occur.
If U is a cone constructed as in Proposition 4.2, then there will be some undetermined subspaces. This construction works in arbitrary dimensions.
The hyperbolic quadric - when the point set U corresponds to the affine part of a hyperbolic quadric which has the ideal hyperplane as a tangent hyperplane - is also a good construction in certain dimensions. Moreover, this works not only if the quadric is hyperbolic, the next paragraphs describe this situation. The question, that whether there are other point sets not determining more than one subspaces or nonsingular quadrics and cones are the only examples, remains open.

Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ be the affine part of a nonsingular quadric which has the ideal hyperplane as a tangent hyperplane (i.e. the intersection of the quadric and the ideal hyperplane is a cone based on an $(n-2)$-dimensional quadric of the same character). Denote by g the projective index of the quadric, i.e. the dimension of the generators, the subspaces of maximum dimension contained in the quadric. Denote by w the character of the quadric, $w = 1,\ 2,\ 0$ for a parabolic, hyperbolic, elliptic quadric, respectively.

In the next proposition we describe the g-dimensional subspaces in H_∞ not determined by U.

Proposition 4.14. *If $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ is defined as above then the undetermined g-dimensional subspaces in H_∞ are exactly the generators contained in the intersection of the quadric and the ideal hyperplane, except the cases when $n = 2$ and q is even, or $n = 4$ and $q = 2$, or $n = 5$ and $q = 2$ and the quadric is elliptic.*

Proof. For the proof we have to mention some basic facts about quadrics.
There are q^{n-1} affine points in the quadric. Consider an arbitrary generator G of the quadric contained in H_∞. There are q^{n-g-1} affine $(g+1)$-dimensional subspaces with the ideal hyperplane G. Each of these $(g+1)$-subspaces contains at most q^g points from the quadric, otherwise the whole $(g+1)$-subspace would be contained in the quadric, which is a contradiction. Since there are q^{n-1} affine points in the quadric, each $(g+1)$-subspace contains exactly q^g points. The intersection of a $(g+1)$-subspace and the quadric is a quadric of dimension $g+1$, containing G, a subspace of dimension g, which is a linear factor. So the rest of the intersection has to be a g-subspace as well. It means that each of the $(g+1)$-dimensional

affine subspaces with the ideal hyperplane G contains exactly an affine g-dimensional subspace from U, so G is undetermined.

On the other hand consider a g-dimensional subspace G' in H_∞ not contained in the quadric. Suppose it is undetermined. It means that each of the q^{n-g-1} $(g+1)$-dimensional affine subspaces with the ideal hyperplane G' contains exactly a g-dimensional subspace from U (i.e. a generator). If the quadric is hyperbolic, such a $(g+1)$-dimensional subspace should contain one more generator (from the other system), contradiction. If the quadric is elliptic or parabolic, the ideal hyperplanes of these generators are in G' and they are of dimension $g-1$. Since G' is not a generator, it can contain at most two $(g-1)$-subspaces from the quadric. This implies that there is a $(g-1)$-subspace in the intersection of G' and the quadric, which is the ideal hyperplane of at least $\frac{q^{n-g-1}}{2}$ generators. The number of generators through a fixed $(g-1)$-subspace is the following:

$\varrho(g-1,n,w) = (q^{2-w}+1)\cdot(q^{2-w+1}+1)\cdot\ldots\cdot(q^{\frac{n-2g+1-w}{2}}+1)$.

For an elliptic quadric $\varrho(\frac{n-5}{2},n,0) = q^2+1 < \frac{q^{\frac{n+1}{2}}}{2}$, if $n\geq 5$ and $q\geq 3$ or $n\geq 7$;
for a parabolic quadric $\varrho(\frac{n-4}{2},n,1) = q+1 < \frac{q^{\frac{n}{2}}}{2}$, if $n\geq 4$ and $q\geq 3$ or $n\geq 6$, contradiction.

If $n=3$, for an elliptic quadric it is clear that through a point in H_∞ not contained in the quadric there are q^2 affine lines, and $q+1$ of them are tangents to the quadric, all the others are secants or skew lines. Since there are q^2 affine points in the quadric, the point at infinity will be determined.

Similarly, if $n=2$, q odd, through a point on ℓ_∞ not contained in the quadric, there is only one affine line which is tangent to the quadric, all the others are secants or skew lines, so the point will be determined.

The restrictions in the theorem are not only technical conditions; in low dimensions there exist exceptional examples. If $n=2$ and q is even, the nucleus of the parabolic quadric is a not determined point on the ideal line, but it is not contained in the quadric. For a parabolic quadric in $\mathrm{PG}(4,2)$ and for an elliptic quadric in $\mathrm{PG}(5,2)$ there exist undetermined lines in H_∞ which are not generators. □

Chapter 5

Resolving sets and semi-resolving sets in finite projective planes

5.1 Introduction

In the last two chapters we investigate some connections of finite geometries with other fields. We examine a graph theoretical question and a combinatorial search problem related to finite projective planes.

This chapter is based on [5], which is a joint work with Tamás Héger. Here we first summarize the main concept of resolving sets and semi-resolving sets of the incidence graph of a finite projective plane, giving the definitions and the results. In the following two sections we prove a theorem regarding the metric dimension of such a graph, and classify the smallest resolving sets of it. For the detailed description of semi-resolving sets (and the proof of the corresponding theorem) see [5] and the Ph.D. thesis of Tamás Héger [35].

For an overview of resolving sets and related topics we refer to the survey of Bailey and Cameron [9]. Regarding these, we follow the notation of [9, 8]. Throughout this chapter, $\Gamma = (V, E)$ denotes a simple connected graph with vertex-set V and edge-set E. For $x, y \in V$, $d(x, y)$ denotes the distance of x and y (that is, the length of the shortest path connecting x and y). $\Pi = (\mathcal{P}, \mathcal{L})$ denotes a finite projective plane with point-set $\mathcal{P}$ and line-set $\mathcal{L}$, and q denotes the order of Π. Sometimes Π_q refers to the projective plane of order q.

Definition 5.1. $S = \{s_1, \ldots, s_k\} \subset V$ is a *resolving set* in $\Gamma = (V, E)$, if the ordered distance lists $(d(x, s_1), \ldots, d(x, s_k))$ are unique for all $x \in V$. The *metric dimension of* Γ, denoted by $\mu(\Gamma)$, is the size of the smallest resolving set in it.

Equivalently, S is a resolving set in $\Gamma = (V, E)$ if and only if for all $x, y \in V$, there

exists a point $z \in S$ such that $d(x,z) \neq d(y,z)$. In other words, the vertices of Γ can be distinguished by their distances from the elements of a resolving set. We say that a vertex v is *resolved* by S if its distance list with respect to S is unique. A set $A \subset V$ is resolved by S if all its elements are resolved by S. If the context allows, we omit the reference to S. Note that the distance list is ordered (with respect to an arbitrary fixed ordering of S), the (multi)set of distances is not sufficient.

Take a projective plane $\Pi = (\mathcal{P}, \mathcal{L})$. Recall that the incidence graph $\Gamma(\Pi)$ of Π is a bipartite graph with vertex classes $\mathcal{P}$ and $\mathcal{L}$, where $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$ are adjacent in Γ if and only if P and ℓ are incident in Π. By a resolving set or the metric dimension of Π we mean that of its incidence graph. In [8], Bailey asked for the metric dimension of a finite projective plane of order q. In Section 5.2 we prove the following theorem using purely combinatorial tools.

Theorem 5.2. *The metric dimension of a projective plane of order $q \geq 23$ is $4q-4$.*

It follows that the highly symmetric incidence graph of a Desarguesian projective plane attains a relatively large *dimension jump* (for definitions and details see the end of Section 5.2).

For the case $q \leq 19$ see the considerations also at the end of Section 5.2.

Section 5.3 is devoted to the description of all resolving sets of a projective plane Π of size $4q-4$ ($q \geq 23$).

One may also try to construct a resolving set for $\Pi = (\mathcal{P}, \mathcal{L})$ the following way: take a point-set $\mathcal{P}_S \subset \mathcal{P}$ that resolves $\mathcal{L}$, and take a line-set $\mathcal{L}_S \subset \mathcal{L}$ that resolves $\mathcal{P}$. Then $S = \mathcal{P}_S \cup \mathcal{L}_S$ is clearly a resolving set. Such a resolving set S is called a *split resolving set*, and $\mathcal{P}_S$ and $\mathcal{L}_S$ are called *semi-resolving sets*. By $\mu^*(\Pi)$ we denote the size of the smallest split resolving set of Π (see [8]). Semi-resolving sets are in tight connection with double blocking sets. We recall the definition.

Definition 0.11. A set B of points is a *double blocking set* in a projective plane Π, if every line intersects B in at least two points. $\tau_2 = \tau_2(\Pi)$ denotes the size of the smallest double blocking set in Π.

We proved that in the Desarguesian projective plane of order q if a semi-resolving set S is small enough, then one can extend it into a double blocking set by adding at most two points to S. This yields the following results.

Theorem 5.3. *Let S be a semi-resolving set in $\mathrm{PG}(2,q)$, $q \geq 3$. Then $|S| \geq \min\{2q+q/4-3, \tau_2(\mathrm{PG}(2,q))-2\}$. If $q \geq 121$ is a square prime power, then $|S| \geq 2q+2\sqrt{q}$.*

Corollary 5.4. *Let $q \geq 3$. Then $\mu^*(\mathrm{PG}(2,q)) \geq \min\{4q + q/2 - 6, 2\tau_2(\mathrm{PG}(2,q)) - 4\}$. If $q \geq 121$ is a square prime power, then $\mu^*(\mathrm{PG}(2,q)) = 4q + 4\sqrt{q}$.*

In order to prove these results we used the polynomial method and the Szőnyi–Weiner-lemma. This part of the common results has already appeared in the Ph.D. thesis of Tamás Héger, we refer to his work for the details; here we have the focus on the theory of resolving sets.

Throughout the chapter when we refer to duality, we simply mean that as the axioms of projective planes are symmetric in points and lines, we may interchange the role of points and lines (e.g., consider a set of lines as a set of points), and if we have a result regarding points, then we have the same (dual) result regarding lines. A finite projective plane is not necessarily isomorphic to its dual, however, $\mathrm{PG}(2,q)$ is.

Considering a set S, a line ℓ is an $(\leq i)$-secant, an $(\geq i)$-secant, or an i-secant to S if ℓ intersects S in at most i, at least i, or exactly i points, respectively.

5.2 Resolving sets in finite projective planes

Note that the distance of two distinct points (lines) is always two, while the distance of a point P and a line ℓ is 1 or 3, depending on $P \in \ell$ or $P \notin \ell$, respectively. Note that the elements of a set S are resolved by S trivially, as there is a zero in their distance lists.

Notation.

- For two distinct points P and Q, let PQ denote the line joining P and Q.
- For a point P, let $[P]$ denote the set of lines through P. Similarly, for a line ℓ, let $[\ell]$ denote the set of points on ℓ. Note that we distinguish a line from the set of points it is incident with.
- Once a subset S of points and lines is fixed, the terms *inner point* and *inner line* refer to the elements of S, while *outer points* and *outer lines* refer to those not in S.
- For a fixed subset S of points and lines we say a line ℓ is skew or tangent to S if $[\ell]$ contains zero or one point from S, respectively. Similarly, we say a point P is not covered or 1-covered by S if $[P]$ contains zero or one line from S, respectively.
- For a subset S of points and lines, let $\mathcal{P}_S = S \cap \mathcal{P}$, $\mathcal{L}_S = S \cap \mathcal{L}$.

Lemma 5.5. *Let $S = \mathcal{P}_S \cup \mathcal{L}_S$ be a set of vertices in the incidence graph of a finite projective plane. Then any line ℓ intersecting $\mathcal{P}_S$ in at least two points (that is, $|[\ell] \cap \mathcal{P}_S| \geq 2$) is resolved*

by S. Dually, if a point P is covered by at least two lines of $\mathcal{L}_S$ (that is, $|[P] \cap \mathcal{L}_S| \geq 2$), then P is resolved by S.

Proof. Let ℓ be a line, $\{P, Q\} \subset [\ell] \cap \mathcal{P}_S$, $P \neq Q$. Then any line e different from ℓ may contain at most one point of $\{P, Q\}$, hence e.g. $P \notin [e]$, hence $d(P, \ell) = 1 \neq d(P, e) = 3$. By duality, this holds for points as well. □

Proposition 5.6. *$S = \mathcal{P}_S \cup \mathcal{L}_S$ is a resolving set in a finite projective plane if and only if the following properties hold for S:*

P1 There is at most one outer line skew to $\mathcal{P}_S$.

P1' There is at most one outer point not covered by $\mathcal{L}_S$.

P2 Through every inner point there is at most one outer line tangent to $\mathcal{P}_S$.

P2' On every inner line there is at most one outer point that is 1-covered by $\mathcal{L}_S$.

Proof. By duality and Lemma 5.5 it is enough to see that S resolves lines not in $\mathcal{L}_S$ that are skew or tangent to $\mathcal{P}_S$. Property 1 (P1) assures that skew lines are resolved. Now take a tangent line $\ell \notin \mathcal{L}_S$. If there were another line e with the same distance list as ℓ's (hence $e \notin \mathcal{L}_S$), both e and ℓ would be tangents to $\mathcal{P}_S$ through the point $[\ell] \cap \mathcal{P}_S$, which is not possible by Property 2 (P2). □

We will usually refer to the above alternative definition, but sometimes it is useful to keep the following in mind.

Proposition 5.7. *$S = \mathcal{P}_S \cup \mathcal{L}_S$ is a resolving set in a finite projective plane if and only if the following properties hold for S:*

PA Through any point P there is at most one outer line not blocked by $\mathcal{P}_S \setminus \{P\}$.

PA' On any line ℓ there is at most one outer point not covered by $\mathcal{L}_S \setminus \{\ell\}$.

Proof. In other words, the Property A claims that on a point $P \in \mathcal{P}_S$ there may be at most one tangent from $\mathcal{L} \setminus \mathcal{L}_S$, while on a point $P \notin \mathcal{P}_S$ there may be at most one skew line. As the intersection point of two skew lines would validate the latter one, Property A is equivalent to Properties 1 and 2 of Proposition 5.6. Dually, the same holds for the properties PA', P1' and P2'. □

Proposition 5.8. *The metric dimension of a projective plane of order $q \geq 3$ is at most $4q - 4$.*

Proof. We give a construction refined from Bill Martin's one of size $4q-1$ (cited in [8]), see Figure 5.1. Let P, Q, and R be three arbitrary points in general position. Let $\mathcal{P}_S = [PQ] \cup [PR] \setminus \{P, Q, R\}$, and let $\mathcal{L}_S = [P] \cup [R] \setminus \{PQ, PR, RQ\}$. We will see that $S = \mathcal{P}_S \cup \mathcal{L}_S$ is a resolving set by checking the criteria of Proposition 5.6.

P1: The only outer line skew to $\mathcal{P}_S$ is RQ.

P1': The only outer point uncovered by $\mathcal{L}_S$ is Q.

P2: As $q \geq 3$, $|[PQ] \cap \mathcal{P}_S| = |[PR] \cap \mathcal{P}_S| = q - 1 \geq 2$. On a point $A \in [PQ] \setminus P, Q$ the only tangent is AR (which is in $\mathcal{L}_S$). On a point $A \in [PR] \setminus P, R$ the only tangent is AQ.

P2': As $q \geq 3$, $|[P] \cap \mathcal{L}_S| = |[R] \cap \mathcal{L}_S| = q-1 \geq 2$. The only point of a line $\ell \in [R] \setminus \{PR, RQ\}$ not covered by $[P]$ is $[\ell] \cap [PQ]$ (which is in $\mathcal{P}_S$). The only uncovered point on a line $\ell \in [P] \setminus \{PQ, PR\}$ is $[\ell] \cap RQ$.

Hence S is a resolving set of size $|\mathcal{P}_S| + |\mathcal{L}_S| = 2q - 2 + 2q - 2 = 4q - 4$. □

Our aim is to show that the metric dimension of a projective plane of order $q \geq 23$ is $4q - 4$, and to describe all resolving sets of that size.

A general assumption: from now on we suppose that $S = \mathcal{P}_S \cup \mathcal{L}_S$ is a resolving set of size $\leq 4q - 4$.

Proposition 5.9. $2q - 5 \leq |\mathcal{P}_S| \leq 2q + 1$, $2q - 5 \leq |\mathcal{L}_S| \leq 2q + 1$.

Proof. Let t denote the number of tangents that are not in $\mathcal{L}_S$. By Property 2, $t \leq |\mathcal{P}_S|$. Recall that there may be at most one skew line that is not in $\mathcal{L}_S$ (Property 1). Then double counting the pairs of $\{(P, \ell) \colon P \in \mathcal{P}_S, P \in [\ell], |[\ell] \cap \mathcal{P}_S| \geq 2\}$ we get $2(q^2+q+1-1-t-|\mathcal{L}_S|) \leq |\mathcal{P}_S|(q+1) - t$, whence

$$q|\mathcal{P}_S| \geq 2(q^2 + q - |\mathcal{L}_S|) - t - |\mathcal{P}_S| \geq 2(q^2 + q - (|\mathcal{L}_S| + |\mathcal{P}_S|)) \geq 2(q^2 - 3q + 4),$$

thus $|\mathcal{P}_S| \geq 2q - 6 + 8/q$, and as it is an integer, $|\mathcal{P}_S| \geq 2q - 5$. Dually, $|\mathcal{L}_S| \geq 2q - 5$ also holds. From $|\mathcal{P}_S| + |\mathcal{L}_S| \leq 4q - 4$ (Proposition 5.8) the upper bounds follow. □

This immediately gives $|S| \geq 4q - 10$. We remark that a somewhat more careful calculation shows $2q - 4 \leq |\mathcal{P}_S| \leq 2q$ and hence $|S| \geq 4q - 8$, provided that $q \geq 11$, but we don't need to use it.

Remark 5.10. The metric dimension of the Fano plane is five.

Proof. Suppose $|\mathcal{P}_S| \leq 2$. Using the notations of the proof of Proposition 5.9, we see $2(7 - 1 - |\mathcal{P}_S| - |\mathcal{L}_S|) \leq |\mathcal{P}_S|$ (as there is at most one two-secant through any point). This yields $|\mathcal{L}_S| \geq 6 - 3|\mathcal{P}_S|/2$, whence $|\mathcal{P}_S| + |\mathcal{L}_S| \geq 6 - |\mathcal{P}_S|/2 \geq 5$. Figure 5.1 shows a resolving set of size five in the Fano plane. □

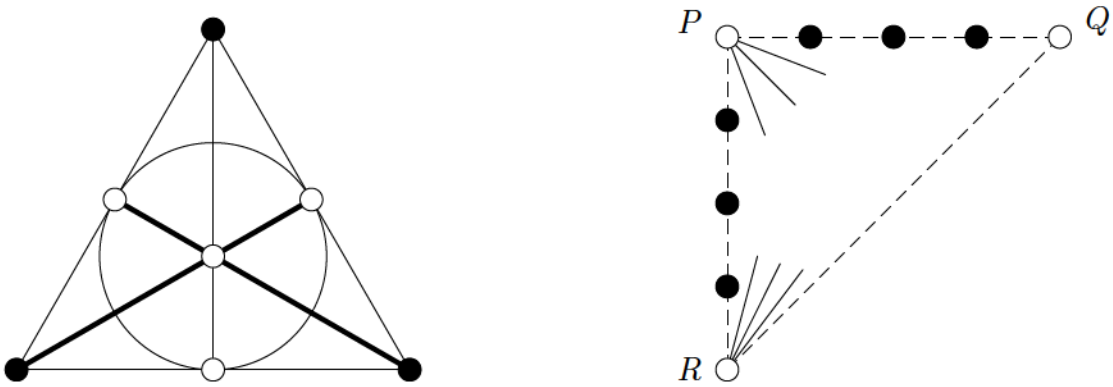

Figure 5.1: On the left the black points and the thick lines form a resolving set of size five in the Fano plane. On the right the black points and the continuous lines form a resolving set of size $4q-4$.

One more general assumption: by duality we may assume that $|\mathcal{P}_S| \leq |\mathcal{L}_S|$. Thus, as $|\mathcal{P}_S| + |\mathcal{L}_S| \leq 4q-4$, $|\mathcal{P}_S| \leq 2q-2$ follows.

Proposition 5.11. *Let* $q \geq 23$. *Then any line intersects* $\mathcal{P}_S$ *in either* ≤ 4 *or* $\geq q-4$ *points.*

Proof. Consider a line ℓ from the projective plane. Suppose that $|[\ell] \cap \mathcal{P}_S| = x$, $2 \leq x \leq q$. For a point $P \in [\ell] \setminus \mathcal{P}_S$, let $s(P)$ and $t(P)$ denote the number of skew or tangent lines to $\mathcal{P}_S$ through P, respectively; moreover, denote by s the number of skew lines, and let t denote the total number of tangents intersecting ℓ outside $\mathcal{P}_S$. Then counting the points of $\mathcal{P}_S$ on ℓ and the other lines through P we get $2q-2 \geq |\mathcal{P}_S| \geq x + t(P) + 2(q - t(P) - s(P))$, equivalently, $x \leq 2s(P) + t(P) - 2$. Adding up the inequalities for all $P \in [\ell] \setminus \mathcal{P}_S$ we obtain

$$(q+1-x)x \leq 2s + t - 2(q+1-x).$$

Now, Proposition 5.6 yields that $s \leq |\mathcal{L}_S| + 1$ and $s + t \leq (1 + |\mathcal{P}_S| - x) + |\mathcal{L}_S|$ (here first we estimate the skew / tangent lines in question that are outside $\mathcal{L}_S$, then the rest), whence $2s + t \leq 2|\mathcal{L}_S| + |\mathcal{P}_S| - x + 2$. Combined with the previous inequality we obtain

$$x^2 - qx + 4q - 3 \geq 0.$$

Assuming $q \geq 23$, the left hand side is negative for $x = 5$ and $x = q-5$, therefore, as x is an integer, we conclude that $x \leq 4$ or $x \geq q-4$. □

Proposition 5.12. *Let* $q \geq 23$. *Then there exist two lines intersecting* $\mathcal{P}_S$ *in at least* $q-4$ *points.*

Proof. By Proposition 5.11 every line is either a ≤ 4 or a $\geq (q-4)$-secant. Suppose to the contrary that every line intersects $\mathcal{P}_S$ in at most 4 points except possibly one line ℓ; let

$x = |[\ell] \cap \mathcal{P}_S| \geq 2$. Note that $x \leq 4$ is also possible. Let n_i denote the number of i-secants to $\mathcal{P}_S$ different from ℓ. To be convinient, let $n_0 = s$ and $n_1 = t$, and let $b = |\mathcal{P}_S|$. Then the standard equations yield

$$\begin{aligned} \sum_{i=2}^{4} n_i &= q^2 + q + 1 - s - t - 1, \\ \sum_{i=2}^{4} i n_i &= (q+1)b - t - x, \\ \sum_{i=2}^{4} i(i-1) n_i &= b(b-1) - x(x-1). \end{aligned}$$

Thus

$$0 \leq \sum_{i=2}^{4} (i-2)(4-i) n_i = -\sum_{i=2}^{4} i(i-1) n_i + 5 \sum_{i=2}^{4} i n_i - 8 \sum_{i=2}^{4} n_i =$$

$$-b^2 + (5q+6)b + x(x-6) + 3(s+t) + 5s - 8(q^2+q).$$

Substituting $s + t \leq |\mathcal{P}_S| + |\mathcal{L}_S| + 1 \leq 4q - 3$, $s \leq |\mathcal{L}_S| + 1 \leq 2q + 2$ and $x \leq q + 1$, we get

$$0 \leq -b^2 + (5q+6)b - 7q^2 + 10q - 4.$$

By duality we assumed $b = |\mathcal{P}_S| \leq 2q-2$. For $b = 2q-2$, the right hand side is $-q^2+20q-20$, which is negative whenever $q \geq 19$. Hence $b > 2q - 2$, a contradiction. □

Now we see that there exist two distinct lines e, f such that $|[e] \cap (\mathcal{P}_S \setminus [e] \cap [f])| = q - l$ and $|[f] \cap (\mathcal{P}_S \setminus [e] \cap [f])| = q - k$ with $k \leq l \leq 5$.

Let $e \cap f = P$ and denote the set of points of $\mathcal{P}_S$ outside $e \cup f$ by Z.

Proposition 5.13. *Suppose $q \geq 23$. Then $k + l \leq 3$. Moreover, $l = 3$ is not possible.*

Proof. Then there are at least $q - 1 - |Z|$ skew or tangent lines through P depending on $P \notin \mathcal{P}_S$ or $P \in \mathcal{P}_S$, respectively, from which at most one may not be in $\mathcal{L}_S$, hence we found $\geq q-2-|Z|$ lines in $[P] \cap \mathcal{L}_S$. Among the $k(q-l)$ lines that connect one of the k points in $[f] \setminus (\mathcal{P}_S \cup \{P\})$ with one of the $q-l$ points in $[e] \cap (\mathcal{P}_S \setminus \{P\})$ at most $k|Z|$ are not tangents to $\mathcal{P}_S$, but through a point in $[e] \cap (\mathcal{P}_S \setminus [e] \cap [f])$, where $|[e] \cap (\mathcal{P}_S \setminus [e] \cap [f])| = q - l$ only one tangent may not be in $\mathcal{L}_S$. Hence we find another $\geq k(q-l) - k|Z| - (q-l) = (k-1)(q-l) - k|Z|$ lines in $\mathcal{L}_S$. Interchanging the role of e and f, we find yet another $\geq (l-1)(q-k) - l|Z|$ lines in $\mathcal{L}_S$. These three disjoint bunches give $|\mathcal{L}_S| \geq (k+l-1)q - (k+l+1)|Z| + (k+l) - 2kl - 2$.

Now as $(q-k) + (q-l) + |Z| \leq |\mathcal{P}_S| \leq 2q - 2$, $|Z| \leq k + l - 2$ holds, whence $|\mathcal{L}_S| \geq (k+l-1)q - (k^2 + l^2 + 4kl - 2(k+l))$.

We want to use that $2kl - 2(k+l) \leq (k+l)^2 - 2(k+l)^{3/2}$, which is equivalent with $k^2 + l^2 \geq 2(k+l)(\sqrt{k+l} - 1)$. As $x \mapsto x^2$ is convex, $k^2 + l^2 \geq 2\left(\frac{k+l}{2}\right)^2 = (k+l)^2/2 \geq 2(k+l)(\sqrt{k+l} - 1)$, where the last inequality follows from $(\sqrt{k+l} - 2)^2 \geq 0$.

Therefore, $k^2 + l^2 + 4kl - 2(k+l) = (k+l)^2 + 2kl - 2(k+l) \leq 2(k+l)^2 - 2(k+l)^{3/2}$, thus $2q + 1 \geq |\mathcal{L}_S| \geq (k+l-1)q - 2(k+l)^2 + 2(k+l)^{3/2}$, hence

$$\frac{2(k+l)^2 - 2(k+l)^{3/2} + 1}{k+l-3} \geq q \geq 23.$$

The left hand side as a function of $k+l$ on the closed interval $[4, 10]$ takes its maximum at $k+l = 10$, and its value is < 20. Hence $k+l < 4$, i.e., $k+l \leq 3$.

Now suppose that $l = 3$ (hence $k = 0$). Recall that we may assume $|\mathcal{P}_S| \leq 2q - 2$, hence $|Z| \leq 1$. Then, as above, the number of lines $\in \mathcal{L}_S$ through P and on the three points in $e \setminus (\mathcal{P}_S \cup \{P\})$ would be at least $q-3+2q-3 = 3q-6$, but $|\mathcal{L}_S| \leq 2q+1$, a contradiction. □

Right now we see that if $q \geq 23$, then there are two lines containing at least $q-1$ and $q-2$ points (which also implies $|\mathcal{P}_S| \geq 2q-3$, hence $|\mathcal{L}_S| \leq 2q-1$ as well). Next we show this dually for lines. The dual arguments of the previous ones would also work, but we used duality to assume $|\mathcal{P}_S| \leq 2q-2$ to keep the technical bound on q as low as possible, hence we make further considerations. Note that at most one point of $\mathcal{P}_S$ may not be covered by e and f, whence Property A yields $|[P] \cap \mathcal{L}_S| \geq q-3$. The following technical lemma holds in general.

Lemma 5.14. *Let e and f be two distinct lines, $\{P\} = [e] \cap [f]$, $\{R_1, \ldots, R_q\} = [e] \setminus \{P\}$, $\{Q_1, \ldots, Q_q\} = [f] \setminus \{P\}$, $L \subset \mathcal{L} \setminus \{[P]\}$. Let $r_i = |L \cap [R_i]|$, $d_i = \max\{|L \cap [Q_i]| - 1, 0\}$, $m = d_1 + \ldots + d_q$. Then for the number C of points in $\mathcal{P} \setminus ([e] \cup [f])$ covered by L,*

$$C \leq |L|(q-1) - r_i(|L| - r_i) + m \leq |L|q - r_i(|L| - r_i + 1)$$

holds, where $i \in \{1, \ldots, q\}$ is arbitrary.

Proof. Without loss of generality we may assume $i = 1$. Let $d(R_j)$ $(2 \leq j \leq q)$ denote the number of lines in $L \cap [R_j]$ that intersect a line of $[R_1] \cap L$ on f. Then $\sum_{j=2}^{q} d(R_j) \leq m$ (count the lines in question through the points of f). Each line through R_1 covers $q-1$ points of $\mathcal{P} \setminus ([e] \cup [f])$, while a line h through R_j $(2 \leq j \leq q)$ covers $q - 1 - r_1 + \varepsilon$ new points, where $\varepsilon = 1$ or 0 depending on whether $h \cap f$ is covered by a line of $[R_1] \cap L$ or not, respectively. Therefore,

$$C \leq r_1(q-1) + \sum_{j=2}^{q} (r_j(q - 1 - r_1) + d(R_j)) = (q-1)\sum_{j=1}^{q} r_j - r_1 \sum_{j=2}^{q} r_j + \sum_{j=2}^{q} d(R_j) \leq$$

$$|L|(q-1) - r_1(|L| - r_1) + m.$$

The second inequality follows immediately from $m \leq |L| - r_1$. □

Proposition 5.15. *There exists a point $R \in [e] \setminus \{P\}$ such that $|([R] \setminus e) \cap \mathcal{L}_S| \geq q-1$. Moreover, if $l = 2$, then $R \notin \mathcal{P}_S$.*

Proof. We use the notations of Lemma 5.14 with $L = \mathcal{L}_S \setminus [P]$. Let $W = \mathcal{P} \setminus [e] \cup [f]$. Suppose to the contrary that

$$r_i < q-1 \text{ for all } 1 \leq i \leq q. \qquad (\star)$$

Case 1: $l = 2$, $k \in \{0,1\}$. $|\mathcal{L}_S| \leq 2q-1$ and $|[P] \cap \mathcal{L}_S| \geq q-3$ implies $|L| \leq q+2$. Keeping in mind that there may be one (but no more) point in $\mathcal{P}_S \cap W$, Property A' for the lines of $[P] \setminus \{e, f\}$ implies that L must cover at least $(q-2)(q-1)+(q-2) = q(q-2)$ points of W. Then by Lemma 5.14, $q(q-2) \leq |L|q - r_i(|L| - r_i + 1) \leq (q+2)q - r_i(q+3-r_i)$ (as the right hand side of the first inequality is growing in $|L|$, since $r_i < q$), which is equivalent with $r_i(q+3-r_i) \leq 4q$. As the left hand side takes its minimum on the interval $[5, q-2]$ in $r_i = 5$ and $r_i = q-2$, substituting $r_i = 5$ yields $q \leq 10$, which does not hold. Hence $r_i \leq 4$ or $r_i \geq q-1$, thus by our assumption $r_i \leq 4$ for all $1 \leq i \leq q$. Recall that $l = 2$. Let R_1 and R_2 be the corresponding two points on $[e] \setminus \mathcal{P}_S$. According to Property A and considering the same ideas as in the proof of Proposition 5.13, we see that at least $q-2$ lines of $[R_1] \cup [R_2]$ must be in L. Thus $q-2 \leq r_1 + r_2 \leq 8$, a contradiction. Therefore, without loss of generality we may conclude that $r_1 \geq q-1$.

Case 2: $k = l = 1$. In this case $\mathcal{P}_S = ([e] \setminus \{P, R\}) \cup ([f] \setminus \{P, Q\})$, and $|\mathcal{P}_S| = |\mathcal{L}_S| = 2q-2$. Note that the role of the lines e and f may be interchanged as they have the same combinatorial properties, thus we may expand the assumption $(\star)$ to f as well, and it is also suitable to find the point R on f. Now $W \cap \mathcal{P}_S = \emptyset$, thus Property A' yields that at least $(q-1)^2$ points of W must be covered by L, moreover, Property A implies $|([P] \setminus \{e, f\}) \cap \mathcal{L}_S| \geq q-2$, whence $|L| \leq q$ follows.

Subcase 2.1: $[P] \setminus (\mathcal{L}_S \cup \{e, f\}) = \{\ell\} \neq \emptyset$. As there may be at most one skew line outside $\mathcal{L}_S$ (Property 1'), this implies that the skew line RQ is in $\mathcal{L}_S$. Lemma 5.14 yields $(q-1)^2 \leq |L|q - r_i(|L| - r_i + 1) \leq q^2 - r_i(q+1-r_i)$, equivalently, $r_i(q+1-r_i) \leq 2q-1$. As in Case 1, this shows that $3 \leq r_i \leq q-2$ is not possible, hence by $(\star)$ $r_i \leq 2$ for all $1 \leq i \leq q$. Interchanging e and f, we see that on any point in $[f] \setminus \{P\}$ there are at most two lines from L, hence $m \leq q/2$. Then again by Lemma 5.14, $(q-1)^2 \leq |L|(q-1) - r_i(|L| - r_i) + m \leq |L|(q-1) - r_i(|L| - r_i) + q/2$, equivalently, $r_i(q - r_i) \leq 3q/2 - 1$, hence $r_i \leq 1$ follows $(1 \leq i \leq q)$. Again, this holds for f as well; that is, every point on $([e] \cup [f]) \setminus \{P\}$ is covered at most once by L. The line RQ is in $\mathcal{L}_S$, but then the points R and Q violate Property 2'.

Subcase 2.2: $[P] \setminus \{e, f\} \subset \mathcal{L}_S$. Then $|[P] \cap \mathcal{L}_S| \geq q-1$, thus $|L| \leq q-1$. Let $i \in \{1, \ldots, q\}$. Recall that $m \leq |L| - r_i$. Combined with Lemma 5.14 we get $(q-1)^2 \leq (q-1)^2 - r_i(q-1-r_i) + m$, therefore $r_i(q-1-r_i) \leq m \leq q-1-r_i$, hence $r_i \leq 1$. As

this is valid for the points of f as well, $m = 0$ follows. But then (under the assumption $(\star)$) $r_i = 0$ would hold for all $1 \leq i \leq q$, which is impossible. □

We have seen that $|([P] \setminus \{e, f\}) \cap \mathcal{L}_S| \geq q - 3$. Now we prove that equality can not hold.

Proposition 5.16. $|([P] \setminus \{e, f\}) \cap \mathcal{L}_S| \geq q - 2$.

Proof. Suppose to the contrary that there exist two distinct lines, g and h, such that $\{g, h\} \subset [P] \setminus \{e, f\}$, $\{g, h\} \cap \mathcal{L}_S = \emptyset$. Property A yields that (at least) one of them is blocked by a point $Z \in (\mathcal{P}_S \setminus \{[e] \cup [f]\})$. Thus $k = 1$, $l = 2$, $P \notin \mathcal{P}_S$ and $|\mathcal{P}_S \setminus \{[e] \cup [f]\}| = 1$. Let R be the point on $[e] \setminus \{P\}$ found in Proposition 5.15. Then $|\mathcal{L}_S \setminus ([P] \cup [R])| \leq 1$, let ℓ denote this (possibly not existing) line. Take a line r of $[R] \setminus \{e\}$ that does not go through any of the points $g \cap \ell$, $h \cap \ell$, and Z. Such a line exists as $q - 3 > 0$. The points $r \cap g$ and $r \cap h$ show that r violates Property A', a contradiction. □

Proposition 5.17. *If* $|\mathcal{P}_S| = 2q - 3$, *then* $|\mathcal{L}_S| \geq 2q - 1$.

Proof. $|\mathcal{P}_S| = 2q - 3$ means that $k + l = 3$. Let R be the point on $[e] \setminus \{P\}$ found in Proposition 5.15, and denote by R' the point $[e] \setminus (\{\mathcal{P}_S\} \cup \{P, R\})$. We count the lines in S:

- By Proposition 5.16 $|([P] \setminus \{e, f\}) \cap \mathcal{L}_S| \geq q - 2$;
- By Property 2 in Proposition 5.6, through any point $F \in [f] \setminus \{P, Q\}$ at least one of the lines FR, FR' has to be in $\mathcal{L}_S$ as both are tangents to $\mathcal{P}_S$ (at least $q - 1$ lines);
- By Property 1 in Proposition 5.6, at least two of the three skew lines $(\ell_0, RQ, R'Q)$ has to be in $\mathcal{L}_S$.

Altogether there are at least $2q - 1$ lines in $\mathcal{L}_S$. □

Thus, due to the assumption $|\mathcal{P}_S| \leq |\mathcal{L}_S|$, either $|\mathcal{P}_S| = 2q - 3$ and $|\mathcal{L}_S| \geq 2q - 1$ or $2q - 2 \leq |\mathcal{P}_S| \leq |\mathcal{L}_S|$. This completes the proof of Theorem 5.2.

Some lower bound on q is necessary in Theorem 5.2. As we have seen, the theorem fails for $q = 2$ (Remark 5.10), since $\mu(\mathrm{PG}(2, 2)) = 5$. By Proposition 5.8 we have $\mu(\mathrm{PG}(2, q)) \leq 4q-4$ for $q \geq 3$. We have checked that $\mu(\mathrm{PG}(2, q)) = 4q - 4$ for $q = 3$ as well; however, the upper bound is not always tight. For $q = 4$, a computer search showed $\mu(\mathrm{PG}(2, 4)) = 10$, and $\mathrm{PG}(2, 5) \leq 15$. We show a nice construction of size ten in $\mathrm{PG}(2, 4)$. For basic facts about hyperovals see [36]. A hyperoval $\mathcal{O}$ in $\mathrm{PG}(2, 4)$ has six points, no tangents, $6 \cdot 5/2 = 15$ secants and six skew lines. Through any point $P \notin \mathcal{O}$ there pass at most two skew lines, otherwise counting the points of $\mathcal{O}$ on the lines through P we obtained $|\mathcal{O}| \leq 4$. Thus the

set $\mathcal{O}^D$ of skew lines form a dual hyperoval. Now let $P \in \mathcal{O}$ and $\ell \in \mathcal{O}^D$ be arbitrary, and let $\mathcal{P}_S = \mathcal{O} \setminus \{P\}$, $\mathcal{L}_S = \mathcal{O}^D \setminus \{\ell\}$, $S = \mathcal{P}_S \cup \mathcal{L}_S$. Clearly, ℓ is the only outer skew line to $\mathcal{P}_S$, and there is precisely one tangent line on every point $R \in \mathcal{P}_S$ (namely PR). Thus P1 and P2 hold. Dually, P1' and P2' also hold, thus S is a resolving set of size ten.

We remark that projective planes show an interesting example of highly symmetric graphs with large dimension jump. Here we follow the notations of [9]. A vertex-set B in a graph Γ is called a *base*, if the only automorphism of Γ that fixes B pointwise is the identity. The size of the smallest base of Γ is called the *base size of* Γ, and it is denoted by $b(\Gamma)$. As a resolving set of Γ is a base, $b(\Gamma) \leq \mu(\Gamma)$ always holds. A repeatedly investigated question asks how large the gap $\delta(\Gamma) = \mu(\Gamma) - b(\Gamma)$ may be between these two parameters, referred to as the *dimension jump of* Γ (see [9] and the references therein). Let Γ be the incidence graph of $\mathrm{PG}(2, q)$. Then Γ has order $n = 2(q^2 + q + 1)$. It is well known that (the automorphism group of) Γ is distance-transitive (that is, any pair (u, v) of vertices can be transferred into any other pair (u', v') of vertices by an automorphism of Γ unless $d(u, v) \neq d(u', v')$.) It is easy to see that $b(\Gamma) \leq 5$ (four points are enough to fix the linear part of the collineation, and one more point forces the field automorphism to be the identity). Thus $\delta(\Gamma) \geq 4q - 9$, which is quite large in terms of the order of Γ, roughly $2\sqrt{2n}$.

5.3 Constructions

Now we describe all resolving sets of size $4q - 4$. Observing the nice symmetry and self-duality of the shown construction in Proposition 5.8, one might think that it is the only construction. However, this could not be further from the truth. In our somehow arbitrarily chosen system, there are 32 different constructions. Recall that we assume $|\mathcal{P}_S| \leq |\mathcal{L}_S|$.

By Propositions 5.13, 5.15 and 5.16, we know that any resolving set $S = \mathcal{P}_S \cup \mathcal{L}_S$ of size $4q-4$ must contain the following structure $S^* = \mathcal{P}_S^* \cup \mathcal{L}_S^*$ of size $4q-6$ (see Figure 5.2): two lines, e, f, where $[e] \cap [f] = \{P\}$, such that $|\mathcal{P}_S^* \cap ([e] \setminus \{P\})| = q-2$, $|\mathcal{P}_S^* \cap ([f] \setminus \{P\})| = q-1$, $|\mathcal{L}_S^* \cap ([P] \setminus \{e, f\})| = q - 2$, and for one of the points in $[e] \setminus (\mathcal{P}_S^* \cup \{P\})$, denote it by R, $|\mathcal{L}_S^* \cap ([R] \setminus \{e\})| = q - 1$. We denote by R' the other point in $[e] \setminus (\mathcal{P}_S^* \cup \{P, R\})$, and let $\{Q\} = [f] \setminus (\mathcal{P}_S^* \cup \{P\})$, $\{\ell_0\} = [P] \setminus (\mathcal{L}_S^* \cup \{e, f\})$, $\{\ell_1\} = [R] \setminus (\mathcal{L}_S^* \cup \{e\})$. If $Q \notin \ell_1$, then let $T = f \cap \ell_1$.

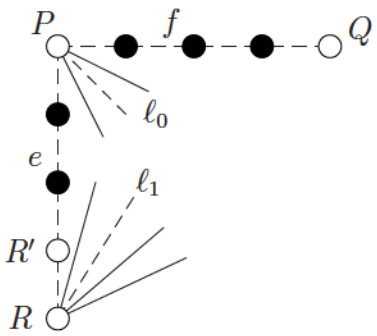

Figure 5.2: The structure S^* of size $4q-6$ that is contained in any resolving set of size $4q-4$.

Here black points and continuous lines refer to the elements of S^*.

We have to complete this structure S^* by adding two more objects to get a resolving set S. Assuming $|\mathcal{P}_S| \leq |\mathcal{L}_S|$, we have to add two lines or one line and one point, and then check the criteria of Proposition 5.6.

The problems of S^* compared to the properties in Proposition 5.6 are the following:

- P1 (outer skew lines to $\mathcal{P}_S^*$): ℓ_0, $R'Q$, and if $Q \in \ell_1$, then ℓ_1.
- P1' (outer points not covered by $\mathcal{L}_S^*$): R', $\ell_0 \cap \ell_1$ and if $Q \in \ell_1$, then Q.
- P2 (outer tangent lines through an inner point): if $Q \notin \ell_1$, then through $T = f \cap \ell_1$ the lines $\ell_1 = RT$ and $R'T$ are tangents. Furthermore, if we add the intersection point of two outer skew lines (listed at P1), those will be two outer tangents through it.
- P2' (outer 1-covered points on an inner line): if $Q \notin \ell_1$, then on RQ the points Q and $\ell_0 \cap RQ$ are 1-covered. Furthermore, if we add the line connecting two outer uncovered points (listed at P1'), those will be two outer one-covered points on it.

These problems must be resolved after adding the two objects. By the letter "C" and a number we refer to the respective part of Figure 5.3 at the end of the chapter. Black points and continuous lines correspond there to the elements of the resolving sets. We distinguish the cases whether we add ℓ_1 into S or not, and whether $Q \in \ell_1$ or not.

I. $\ell_1 \in \mathcal{L}_S$ (see Figure 5.3 (a)).

Now the problems of this construction compared to the properties are the following:

- P1: ℓ_0, $R'Q$.
- P1': solved automatically, as the only outer not covered point is R'.

- P2: if we add $\ell_0 \cap R'Q$, then ℓ_0 and $R'Q$ are tangents through it.
- P2': on RQ the points Q and $\ell_0 \cap RQ$ are 1-covered.

Note that in this case it does not matter whether Q was on ℓ_1 or not (see constructions C1-C4 on Figure 5.3). We can add one more line or one point to S to solve these problems.

1.a) Adding ℓ_1 and one more line: in this case P2 is also solved automatically. To solve P1, we have to add one of the skew lines ℓ_0 and $R'Q$. This automatically solves P2' as one of these lines covers one of the 1-covered points on RQ (Q, $\ell_0 \cap RQ$). So we get two constructions: we can add ℓ_0 and ℓ_1 (C1), or $R'Q$ and ℓ_1 (C2).

1.b) Adding ℓ_1 and a point: because of P2, we cannot add the point $\ell_0 \cap R'Q$, so P2 is solved. To solve P1, we have to add a point on ℓ_0 or $R'Q$. To solve P2', we have to add Q (C3) or $\ell_0 \cap RQ$ (C4). Both choices will solve P1.

From now on we do not add ℓ_1 to $\mathcal{L}_S$. We distinguish the cases whether $Q \in \ell_1$ or not.

II. $\ell_1 \notin \mathcal{L}_S$, $Q \in \ell_1$ (see Figure 5.3 (b)).

Now the problems are the following:

- P1: ℓ_0, $R'Q$ and ℓ_1.
- P1': R', $\ell_0 \cap \ell_1$ and Q.
- P2: we have to be careful if we add the intersection of two skew lines (listed at P1).
- P2': we have to take care if we add the line joining two of the uncovered points (listed at P1').

2.a) Adding two lines: to solve P1, we have to add the skew lines ℓ_0 and $R'Q$. But then we cannot solve P2', because Q and R' are two 1-covered points on $R'Q$. So there are no such constructions.

2.b) Adding a point and a line: to solve P1', we have to add or cover at least two of the points Q, R' and $\ell_0 \cap \ell_1$. We cannot do this only by covering two points with a line, because then we cannot solve P2'. So we have to add one of these points.

1. Adding the point Q: P1 is solved automatically, as the only outer skew line is ℓ_0. To solve P2, we have to add $R'Q$, since $R'Q$ and $\ell_1 = RQ$ are outer tangent lines through Q. This solves P1' by covering R'. P2' is solved, as the only outer point on $R'Q$ is R'.
2. Adding the point R': to solve P1, we have to add ℓ_0. This solves P1', as ℓ_0 covers $\ell_0 \cap \ell_1$. P2 and P2' are solved automatically. (This construction was the original example in the proof of Proposition 5.8.)

3. Adding the point $\ell_0 \cap \ell_1$: to solve P1', we have to cover R' or Q. To solve P2, we have to add ℓ_0, as ℓ_0 and ℓ_1 are outer tangent lines through the intersection point. But ℓ_0 does not cover either R' or Q, so there is no such a construction.

So we get two constructions: we can add Q and $R'Q$ (C5) or R' and ℓ_0 (C6).

Remark. We already have two constructions such that S contains Q. In fact if we add Q to $\mathcal{P}_S$ these are the only possibilities. To solve P2, we have to add ℓ_1 or $R'T$, and these are the constructions in 1.b) and 2.b), respectively. So from now on we do not add Q to $\mathcal{P}_S$, and suppose that $Q \notin \ell_1$.

III. $\ell_1 \notin \mathcal{L}_S$, $Q \notin \ell_1$, $Q \notin \mathcal{P}_S$ (see Figure 5.3 (c)).

The problems of this construction compared to the properties are the following:

- P1: ℓ_0 and $R'Q$.
- P1': R' and $\ell_0 \cap \ell_1$.
- P2: (i) through $T = f \cap \ell_1$ the lines $\ell_1 = RT$ and $R'T$ are tangents; (ii) furthermore, we have to be careful if we add $\ell_0 \cap R'Q$.
- P2': (i) on RQ the points Q and $\ell_0 \cap RQ$ are 1-covered; (ii) furthermore, we have to take care if we add the line joining R' and $\ell_0 \cap \ell_1$.

3. Adding two lines ($\ell_1 \notin \mathcal{L}_S$, $Q \notin \mathcal{P}_S$, $Q \notin \ell_1$): to solve P1, we have to add ℓ_0 or $R'Q$. This automatically solves P1' by covering $\ell_0 \cap \ell_1$ or R'; and also solves P2'(i) by covering $\ell_0 \cap RQ$ or Q. To solve P2, we have to add $R'T$. P2'(ii) could be a problem if we add $R'Q$ and $(\ell_0 \cap \ell_1) \in R'Q$, but adding $R'T$ solves it as well by covering R'. So we get two new constructions: we can add ℓ_0 and $R'T$ (C7) or $R'Q$ and $R'T$ (C8).

From now on we have to add a point and a line to S.

Notation. Let U be an arbitrary point in $\{[e] \setminus \{P, R, R'\}\}$, and V in $\{[f] \setminus \{P, Q, T\}\}$. Note that $U, V \in \mathcal{P}_S^*$.

Since most of the problems are caused by R', we distinguish the cases whether we add R' to $\mathcal{P}_S$ or not.

4. Adding R' to $\mathcal{P}_S$ ($\ell_1 \notin \mathcal{L}_S$, $Q \notin \mathcal{P}_S$, $Q \notin \ell_1$): P1 is solved as the only outer skew line to $\mathcal{P}_S$ is ℓ_0. P1' is solved as the only outer point not covered by $\mathcal{L}_S$ is $\ell_0 \cap \ell_1$. P2 is solved as through T the only outer tangent line is ℓ_1. The new line cannot cause problem compared to P2'(ii) as R' is an inner point now. The only problem we have to solve is P2'(i): on RQ we have to cover Q or $\ell_0 \cap RQ$ with a line.

1. Q: We can cover it by f (C9) or UQ (C10), both choices solve P2'.

2. $\ell_0 \cap RQ$: We can cover it by ℓ_0 (C11) or the line connecting U and $\ell_0 \cap RQ$ (C12), both choices solve P2'.

From now on we suppose that $R' \notin \mathcal{P}_S$.

IV. $\ell_1 \notin \mathcal{L}_S$, $Q \notin \ell_1$, $Q \notin \mathcal{P}_S$, $R' \notin \mathcal{P}_S$ (see Figure 5.3 (b)), we add one point and one line.

As we have to add a point and a line to S, we will go through sistematically the possible addable lines keeping in mind the assumptions. First we check the line e, and then the lines which go through the points of $[e]$. We have to distinguish the points P, $U \in [e] \cap \mathcal{P}_S^*$ and R' (as we have already seen the case adding ℓ_1, the only outer line through R). We continue to refer to the problems listed in the case **III.** Note that P2'(ii) causes problem only in the last case (when adding a line through R').

5. Adding e to $\mathcal{L}_S$: P1' is solved as e covers R'. To solve P2'(i), we have to add $\ell_0 \cap RQ$ (as we do not add Q); this also solves P1. $\ell_0 \cap \ell_1 \notin RQ$ so this solves P2 only if $\ell_0 \cap RQ \in R'T$ (C13).

6. Adding a line through P:

6. a) Adding f: P2'(i) is solved as f covers Q. To solve P1', we have to add $\ell_0 \cap \ell_1$ (as we do not add R'); this also solves P1 and P2(i). By P2(ii), this works only if $\ell_0 \cap \ell_1 \notin R'Q$ (C14).

6. b) Adding ℓ_0: P1 and P1' are solved as the only outer skew line and outer not covered point are $R'Q$ and R'. P2'(i) is solved as ℓ_0 covers $\ell_0 \cap RQ$. To solve P2, we have to add an arbitrary point Z on one of the lines ℓ_1 (C15) and $R'T$ (C16). Note that in the former case we may add the point R as well.

7. Adding a line through U: we have to distinguish whether the added line meets f in a point $V \in \{[f] \setminus \{P, Q\}\}$ or in Q. (Here we do not have to take care of T, the problems are the same for UV and UT.)

7. a) Adding UV: as UV does not cover R' and Q, and we do not add these points to S, to solve P1' and P2', one of the points $\ell_0 \cap \ell_1$ and $\ell_0 \cap RQ$ has to be covered by UV, and the other one has to be added to S. If UV contains $\ell_0 \cap \ell_1$ and we add $\ell_0 \cap RQ$, then P1' and P2' are solved, as well as P1. This solves P2 only if $\ell_0 \cap RQ \in R'T$ (C17). If UV contains $\ell_0 \cap RQ$ and we add $\ell_0 \cap \ell_1$, then P1', P2', P1 and P2(i) are solved. By P2(ii) this works only if $\ell_0 \cap \ell_1 \notin R'Q$ (C18).

7. b) Adding UQ: P2' is solved. If $\ell_0 \cap \ell_1 \notin UQ$, then we have to add $\ell_0 \cap \ell_1$ to solve P1', which also solves P1 and P2(i). By P2(ii), this works only if $\ell_0 \cap \ell_1 \notin R'Q$ (C19). If $\ell_0 \cap \ell_1 \in UQ$, then P1' is solved. To solve P1, we have to add a point on ℓ_0 or on $R'Q$; to solve P2, we have to add point on ℓ_1 or on $R'T$. By P2(ii), we cannot add $\ell_0 \cap R'Q$. Thus we may add $\ell_0 \cap \ell_1$ (C20), $\ell_0 \cap R'T$ (C21) or $\ell_1 \cap R'Q$ (C22). Each choice will solve P1 and

P2.

Now we check the cases when we add a line through R'. This solves P1' as R' will be covered. Because of P2'(ii), we have to distinguish whether the added line contains $\ell_0 \cap \ell_1$ or not.

8. Adding the line g connecting R' and $\ell_0 \cap \ell_1$: to solve P2'(ii), we have to add $\ell_0 \cap \ell_1$. As g cannot contain $\ell_0 \cap RQ$, it has to contain Q to solve P2'(i). This also solves P1 and P2. So we get one construction: if $\ell_0 \cap \ell_1 \in R'Q$, we add $R'Q$ and $\ell_0 \cap \ell_1$ (C23).

9. Adding a line through R' not containing $\ell_0 \cap \ell_1$:

We have to distinguish whether the added line meets f in a point $V \in \{[f] \setminus \{P, T, Q\}\}$, in T or in Q.

9. a) Adding $R'V$: if $\ell_0 \cap RQ$ is not covered by $R'V$, we have to add it to S in order to solve P2'(i). This solves P1, but solves P2 only if $\ell_0 \cap RQ \in R'T$ (C24). If $\ell_0 \cap RQ \in R'V$, then it solves P2'(i). To solve P1, we have to add a point on ℓ_0 or $R'Q$; to solve P2, we have to add a point on ℓ_1 or $R'T$, but we cannot add $\ell_0 \cap R'Q$ because of P2(ii). Adding $\ell_0 \cap R'T$ solves P1 and P2 without any further conditions (C25). Adding $\ell_0 \cap \ell_1$ (C26) or $\ell_1 \cap R'Q$ (C27) solves P1, but by P2(ii), it works only if $\ell_0 \cap \ell_1 \notin R'Q$.

9. b) Adding $R'T$: P2(i) is solved. As $\ell_0 \cap \ell_1 \notin R'T$, P2'(ii) does not cause a problem. If $\ell_0 \cap RQ \notin R'T$, we have to add it to S to solve P2'(i). This solves P1 as well (C28). If $\ell_0 \cap RQ \in R'T$, then P2'(i) is solved. To solve P1, we have to add an arbitrary point Z on ℓ_0 (C29) or on $R'Q$ (C30) except the point $\ell_0 \cap R'Q$. Note that we may add the point $P \in \ell_0$ as well.

9. c) Adding $R'Q$: recall that $\ell_0 \cap \ell_1 \notin R'Q$. P1, P2' and P2(ii) are solved. To solve P2(i), we may add an arbitrary point Z on ℓ_1 (C31) or on $R'T$ (C32). Note that we may also add the point R on ℓ_1.

These are the all possibilities to get a resolving set of size $4q - 4$ assuming $|\mathcal{P}_S| \leq |\mathcal{L}_S|$. There are four constructions with $|\mathcal{P}_S| > |\mathcal{L}_S|$, the duals of (C1), (C2), (C7) and (C8).

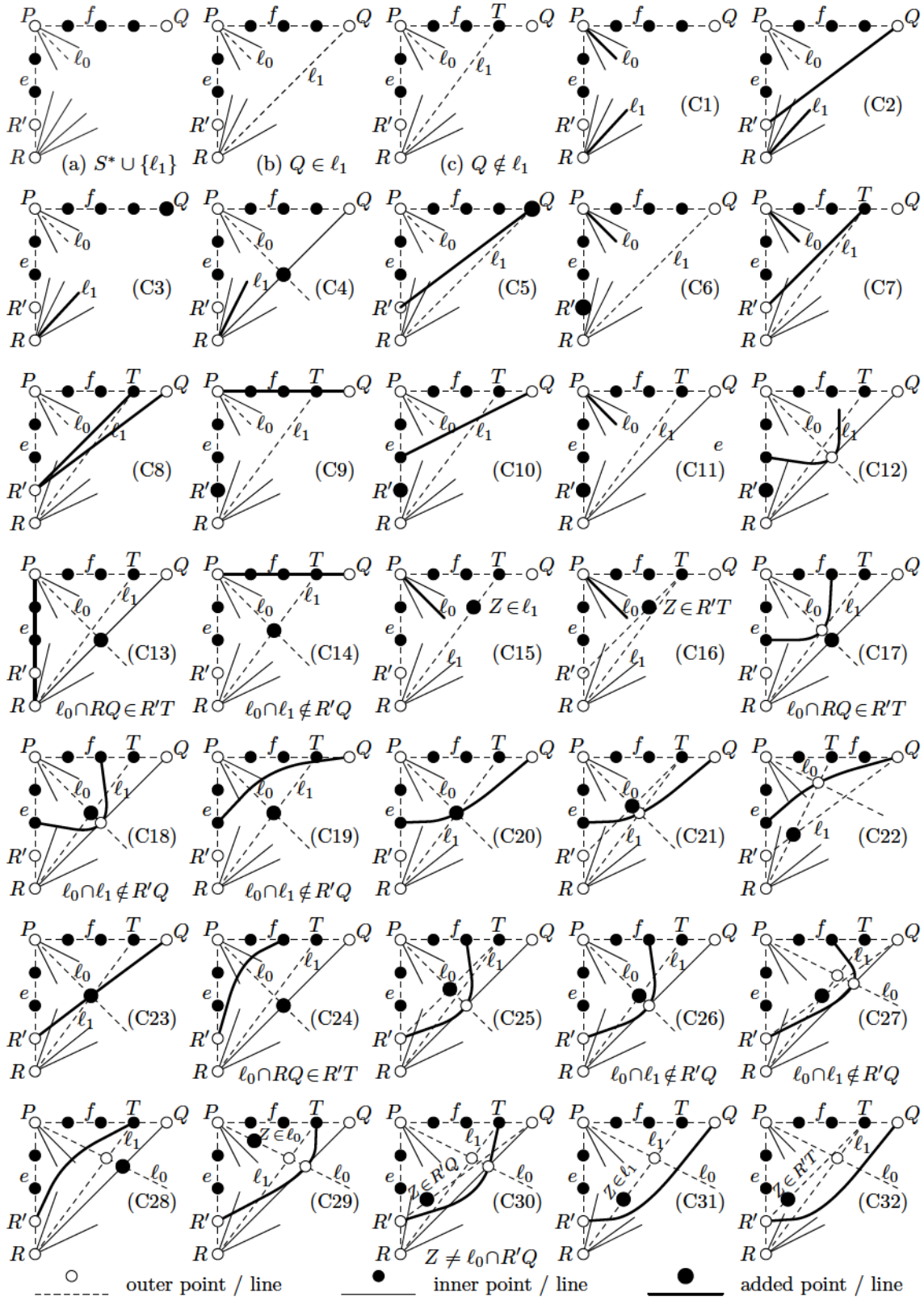

Figure 5.3: The 32 types of resolving sets of size $4q - 4$.

Chapter 6

Search problems in vector spaces

6.1 Introduction

This chapter is based on [6].

Notation. Throughout the chapter log denotes the logarithm of base 2. 1-dimensional subspaces will be denoted by boldface lower case letters, vectors will be denoted by lower case letters with normal typesetting and upper case letters will denote subspaces of higher or unknown dimension.

The starting point of combinatorial search theory is the following problem: given a set X of n elements out of which one x is marked, what is the minimum number s of queries of the form of subsets $A_1, A_2, \ldots, A_s$ of X such that after getting to know whether x belongs to A_i for all $1 \leq i \leq s$ we are able to determine x. Since decades, the number s is known to be equal to $\lceil \log n \rceil$ no matter if the ith query might depend on the answers to the previous ones (*adaptive search*) or we have to ask our queries at once (*non-adaptive search*).

There are lots of variants of this problem. There can be multiple marked elements and our aim can be to determine at least one of them or all of them or a constant fraction of them. The number of marked elements can be known or unknown. There can be restrictions on the possible set Q of queries; only small subsets can be asked or other restrictions may apply. Also, there are models in between the adaptive and the non-adaptive version: we might be allowed to ask our queries in r *rounds*, that is our queries of the $i+1$st round may depend on the answers to all queries in the first i rounds and we would like to minimize the total number of queries. For these and further models we refer the reader to the monograph of Du and Hwang [29].

In this chapter we address the q-analogue of the basic problem. As usual, let q be a prime power and GF(q) the finite field of q elements. Let V denote an n-dimensional vector space over GF(q) and let $\mathbf{v}$ be a marked 1-dimensional subspace of V. We will be interested

in determining the minimum number of queries that is needed to find $\mathbf{v}$ provided all queries are subspaces of V and the answer to a query U is YES if $\mathbf{v} \leqslant U$ and NO if $\mathbf{v} \not\leqslant U$. This number will be denoted by $A(n,q)$ in the adaptive case and $M(n,q)$ in the non-adaptive case. Note that a set $\mathcal{U}$ of subspaces of V can be used as query set to determine the marked 1-space in a non-adaptive search if and only if for every pair $\mathbf{u}, \mathbf{v}$ of 1-subspaces of V there exists a subspace $U \in \mathcal{U}$ with $\mathbf{u} \leqslant U, \mathbf{v} \not\leqslant U$ or $\mathbf{u} \not\leqslant U, \mathbf{v} \leqslant U$. Such systems of subspaces are called *separating*.

Note that the q-analogue problem fits into the original subset settings. Indeed, let the set of k-dimensional subspaces of an n-dimensional vector space V over $\mathrm{GF}(q)$ be denoted by $\begin{bmatrix} V \\ k \end{bmatrix}$. Its cardinality $\left|\begin{bmatrix} V \\ k \end{bmatrix}\right|$ is

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}.$$

Then if we let the underlying set X be $\begin{bmatrix} V \\ 1 \end{bmatrix}$ and the set Q of allowed queries be

$$\left\{ F \subset \begin{bmatrix} V \\ 1 \end{bmatrix} : \exists U \leq V \text{ with } F = \left\{ \mathbf{u} \in \begin{bmatrix} V \\ 1 \end{bmatrix} : \mathbf{u} \leq U \right\} \right\},$$

then we obtain the same problem.

Let us note that it is easy to show that $A(n,2) = M(n,2) = n$ for all $n \geq 2$. We will describe the one line proof in Section 6.3. Thus we will mainly focus on the case when $q \geq 3$.

As usual, the subspaces of an n-dimensional vector space over $\mathrm{GF}(q)$ are considered as the elements of the Desarguesian projective geometry $\mathrm{PG}(n-1,q)$. In Section 6.2 we examine the case when n equals 3, that is the case of projective planes. We determine $A(3,q)$ for all prime powers q.

Theorem 6.1. *Consider a projective plane Π_q of order q. Let $A(\pi_q)$ denote the minimum number of queries in adaptive search that is needed to determine a point of Π_q provided the queries can be either points or lines of π_q. With this notation we have $A(\Pi_q) \leq 2q-1$; if q is a prime power, then $A(\mathrm{PG}(2,q)) = 2q-1$, that is the equality $A(3,q) = 2q-1$ holds.*

In Section 6.2, we also address the problem of determining $M(3,q)$. We obtain upper and lower bounds but not the exact value except if $q \geq 121$ is a square. The most important consequence of our results is the following theorem that states that the situation is completely different from that in the subset case where adaptive and non-adaptive search require the same number of queries.

Theorem 6.2. *For $q \geq 9$ the inequality $A(3,q) < M(3,q)$ holds.*

In Section 6.3, we address the general problem of giving upper and lower bounds on $A(n,q)$ and $M(n,q)$. Our main results are the following theorems.

Theorem 6.3. *For any prime power $q \geq 2$ and positive integer n the inequalities* $\log \begin{bmatrix} n \\ 1 \end{bmatrix}_q \leq A(n,q) \leq (q-1)(n-1)+1$ *hold.*

Theorem 6.4. *There exists an absolute constant $C > 0$ such that for any positive integer n and prime power q the inequalities $\frac{1}{C}q(n-1) \leq M(n,q) \leq 2q(n-1)$ hold. Moreover, if q tends to infinity, then $(1-o(1))q(n-1) \leq M(n,q)$ holds.*

We finish the Introduction by recalling the standard method to prove upper and lower bounds for adaptive search. In both cases we assume the existence of an Adversary. When showing a lower bound b for the number of queries needed to determine the marked element, we have to come up with a strategy that ensures that no matter what sequence of $b-1$ queries the Adversary asks we are able to answer these queries such that there exist at least two elements that match the answers given. In this way we make sure that $b-1$ queries are insufficient. When proving an upper bound our and the Adversary's roles change and this time our task is to provide a strategy using at most b queries (depending on the answers of the Adversary) such that there exists exactly one element that matches the answers no matter what these answers are.

6.2 Projective planes, the case $n = 3$

In this section we prove Theorem 6.1 and Theorem 6.2. Before describing the proofs let us recall some terminology. Π_q denote a projective plane of order q with point set $\mathcal{P}$ and line set $\mathcal{L}$. Remember Definition 0.10: a point set B is called a *blocking set* in Π_q if $|B \cap \ell| \geq 1$ for any line $\ell \in \mathcal{L}$. A point P of a blocking set B is said to be *essential* if $B \setminus \{P\}$ is not a blocking set. A set $\mathcal{C}$ of lines *covers* Π_q if $\cup_{\ell \in \mathcal{C}} \ell = \mathcal{P}$. A line ℓ of a cover $\mathcal{C}$ is *essential* if $\mathcal{C} \setminus \{\ell\}$ is not a cover. A line ℓ is said to be a *tangent* to a set $S \subseteq \mathcal{P}$ if $|\ell \cap S| = 1$ holds. Our main tool in proving Theorem 6.1 is the following result.

Theorem 6.5 (Blokhuis, Brouwer [16])**.** *Let S be a blocking set in* $\mathrm{PG}(2,q)$*. Then there are at least $2q+1-|S|$ distinct tangents to S through any essential point of S.*

This result is actually the same as a unique reducibility theorem of Szőnyi [51]; for more details, we refer to [34, 7]. To obtain Corollary 6.6 from Theorem 6.5 observe that its statement is the dual of Theorem 6.5.

Corollary 6.6. *Let L be a set of covering lines in* $\mathrm{PG}(2,q)$ *and let ℓ be an essential line of L. Then the inequality $|\ell \setminus \cup_{\ell' \neq \ell, \ell' \in L} \ell'| \geq 2q+1-|L|$ holds.* □

Now we recall and prove Theorem 6.1.

Theorem 6.1. *Consider a projective plane Π_q of order q. Let $A(\Pi_q)$ denote the minimum number of queries in adaptive search that is needed to determine a point of Π_q provided the queries can be either points or lines of Π_q. With this notation we have $A(\Pi_q) \leq 2q-1$; if q is a prime power, then $A(\mathrm{PG}(2,q)) = 2q-1$, that is the equality $A(3,q) = 2q-1$ holds.*

Proof. To obtain the upper bound, let us consider the following simple algorithm. Let x be an arbitrary point of the plane and let $\ell_1, \ell_2, \ldots, \ell_{q+1}$ be the lines containing x. Let us ask $\ell_1, \ldots, \ell_q$ one after the other. Once the Adversary answers YES, then we have to find the unknown point on that particular line, this takes at most q further queries. Moreover, if the YES answer comes to a query ℓ_i with $i > 1$, then we only need at most $q-1$ queries as we already know that x is not the unknown point. Thus if a YES answer comes to the ith query, $1 \leq i \leq q$, we are done using $1+q$ or $i+q-1 \leq 2q-1$ queries according to whether $i = 1$ or $i > 1$. If all answers are NO, then we obtain that the unknown point is in $\ell_{q+1} \setminus \{x\}$ and thus we need at most $q+q-1 = 2q-1$ queries.

To obtain the lower bound let us assume first that the Adversary only asks lines as queries. Note that our only choice is about when to say YES for the first time. Indeed, if the queries are $\ell_1, \ell_2, \ldots, \ell_k$ and ℓ_k is the first query which we answer with YES, then the best we can do from then on is to say NO as many times as possible. As the only possibilities for the unknown point are the points in $\ell_k \setminus \cup_{i=1}^{k-1} \ell_i$, therefore the maximum number of queries we can reach is $k + |\ell_k \setminus \cup_{i=1}^{k-1} \ell_i| - 1$.

Our strategy is simple: let the kth query ℓ_k be the first one we answer with YES if there exists a line ℓ such that $\ell_1, \ell_2, \ldots, \ell_k, \ell$ form a covering set of lines. Observe that if an Adversary is able to identify the unknown point, then he must have received a YES answer from us. Indeed, if not, then by our strategy, there would be more than two points that are not contained in any of the lines and thus undistinguishable. Let the kth be the first query to which we answered YES. Then there exists a line ℓ such that $\ell_1, \ell_2, \ldots, \ell_k, \ell$ cover the projective plane. We claim that ℓ_k is essential. Indeed, if not then we should have answered YES earlier. Therefore, Corollary 6.6 applies with ℓ_k being an essential line of the covering set $\{\ell_1, \ell_2, \ldots, \ell_k, \ell\}$. Thus, by our observation in the previous paragraph, the minimum number of queries needed is

$$k + |\ell_k \setminus \cup_{i=1}^{k-1} \ell_i| - 1 \geq k + |\ell_k \setminus (\cup_{i=1}^{k-1} \ell_i \cup \ell)| - 1 \geq k + 2q + 1 - (k+1) - 1 = 2q - 1.$$

Let us now consider the general case where the Adversary is allowed to ask queries that are points. We will always try to replace a point query by a line. If the kth query is a point P_k and there is a line ℓ_k containing P_k such that all previously queried lines and the lines that replaced queried points cannot be extended by a single line to a cover, then we answer NO and provide the additional information to the Adversary that the unknown point does

not lie in ℓ_k. Following this strategy when the Adversary asks a line and with one additional line we can obtain a cover, the reasoning of the previous paragraph goes through.

It remains to check the case when a point P_k is asked and for all lines $P_k \in \ell \notin L = \{\ell_1, \ell_2, \ldots, \ell_{k-1}\}$ there exists another line ℓ' such that $L \cup \{\ell, \ell'\}$ is a cover. In this case we may assume that $P_k \notin \ell'$ for the following reasons. Suppose not and P_k is the unique intersection point of ℓ and ℓ'. Then as neither $L \cup \{\ell\}$ nor $L \cup \{\ell'\}$ is a cover, there must exist points $Q_1 \in \ell \setminus (\cup_{\ell'' \in L} \ell'' \cup \{P_k\}), Q_2 \in \ell' \setminus (\cup_{\ell'' \in L} \ell'' \cup \{P_k\})$. Now for any line $\ell''' \neq \ell, \ell'$ that contains P_k the line ℓ^* that extends $L \cup \{\ell'''\}$ to a cover must contain Q_1 and Q_2 and thus $\ell^* = \langle Q_1, Q_2 \rangle$ and clearly $P_k \notin \langle Q_1, Q_2 \rangle$.

It also follows that ℓ^* is essential in the cover $L \cup \{\ell''', \ell^*\}$, thus if we answer NO to the query P_k and provide the additional information that the unknown point lies in ℓ^*, then the calculation for the restricted case gives us the desired lower bound. □

Let us now turn to the non-adaptive case. The following lemma states that it is enough to consider separating systems consisting of only lines.

Lemma 6.7. *For any separating system S of a projective plane Π, there exists another one S' that contains only lines and $|S| = |S'|$ holds.*

Proof. It is enough to prove the statement for minimal separating systems. Let S be such a system such that it contains the minimum number of points. If this number is 0, then we are done. Suppose S contains a point P. By minimality of S, we know that $S \setminus \{P\}$ is not separating. Clearly, P only separates pairs of points one of which is P itself. There exists exactly one point $Q \neq P$ such that $S \setminus \{P\}$ does not separate the pair (P, Q). Indeed, by the above there is at least one such point, furthermore if there was one more point Q', then Q and Q' would not even be separated by S. Let ℓ be any line containing P and not containing Q. Then $S' = S \setminus \{P\} \cup \ell$ is a separating system such that S' contains one point less than S. This contradicts the choice of S. □

Now we evoke the main concept of the previous chapter and show its connection with the present topic. In a graph G a subset $H_1 \subset V(G)$ of vertices *resolves* another subset H_2 if the list of path-distances in G from the vertices in H_1 are unique in H_2, i.e. for any $h_2, h_2' \in H_2$ there exists an $h_1 \in H_1$ such that $d_G(h_1, h_2) \neq d_G(h_1, h_2')$ holds. A set R of vertices is a *resolving set* in G if it resolves $V(G)$.

If G is bipartite with classes A and B, then a subset A' of A (B' of B) is *semi-resolving* if it resolves B (A). Let G_Π be the incidence graph of a projective plane Π. Then by Lemma 6.7 the minimum size of a separating system in Π equals the minimum size of a semi-resolving set in G_Π. We have seen that the minimum size of a resolving set in any

projective plane of order $q \geq 23$ is $4q - 4$ and we have also mentioned the following lower bound on the size of any semi-resolving set in the incidence graph of $\mathrm{PG}(2, q)$. Remember that $\tau_2(\Pi)$ denotes the minimum size of a *double (2-fold) blocking set* in Π (i.e. the minimum size of a point set in Π that meets every line of Π in at least 2 points).

Theorem 5.3. *Let S be a semi-resolving set in* $\mathrm{PG}(2, q)$, $q \geq 3$. *Then* $|S| \geq \min\{2q + q/4 - 3, \tau_2(\mathrm{PG}(2, q)) - 2\}$.

Theorem 5.3 together with the following theorem implies Theorem 6.2.

Theorem 6.8 (Ball, Blokhuis [13])**.** *Let $q \geq 9$. Then $\tau_2(\mathrm{PG}(2, q)) \geq 2(q + \sqrt{q} + 1)$, and equality holds if and only if q is a square.*

On the other hand, Bailey [8] gave a semi-resolving set of size $\tau_2(\mathrm{PG}(2, q)) - 1$, and in [5] we constructed one of size $2(q + \sqrt{q})$ in $\mathrm{PG}(2, q)$, q a square prime power.

Corollary 6.9. *Let $q \geq 121$ be a square. Then $M(3, q) = 2q + 2\sqrt{q}$ holds.* □

Recall that $A(3, q) = 2q - 1$ by Theorem 6.1. Thus Corollary 6.9 and Theorem 6.1 together prove Theorem 6.2, which we recall below.

Theorem 6.2. *For $q \geq 9$ the inequality $A(3, q) < M(3, q)$ holds.*

The exact value of $\tau_2(\mathrm{PG}(2, q))$ is not known in general. If $q > 3$ is a prime, then Ball proved $\tau_2(\mathrm{PG}(2, q)) \geq 2.5(q + 1)$ [10]. As for large square values of q we have $M(3, q)/q = 2 + 2/\sqrt{q}$, while for prime values of q we have $M(3, q)/q > 2.5$, we obtain the following.

Theorem 6.10. *The sequence $M(3, q)/q$ does not have a limit.* □

In case of $q = p^{2d+1}$, p prime, $d \geq 1$, Blokhuis, Storme and Szőnyi [17] obtained the lower bound $\tau_2(\mathrm{PG}(2, q)) \geq 2(q + 1) + c_p q^{2/3}$, where $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ otherwise. As for an upper bound if q is not a square, Bacsó, Héger and Szőnyi [7] showed $\tau_2(\mathrm{PG}(2, q)) \leq 2q + 2(q - 1)/(r - 1)$, where $q = r^d$, r an odd prime power, d odd. Thus for such parameters, Theorem 5.3 implies that if $r \geq 11$, then $M(3, q)$ is either $\tau_2(\mathrm{PG}(2, q)) - 1$ or $\tau_2(\mathrm{PG}(2, q)) - 2$.

6.3 General bounds

In this section we recall and prove Theorem 6.3 and Theorem 6.4.

Theorem 6.3. *For any prime power $q \geq 2$ and positive integer n the inequalities* $\log \begin{bmatrix} n \\ 1 \end{bmatrix}_q \leq A(n, q) \leq (q - 1)(n - 1) + 1$ *hold.*

Proof. Let us begin with the lower bound as it follows from the trivial lower bound that any separating system of subsets of X should contain at least $\lceil \log |X| \rceil$ sets. Therefore any separating system of subspaces of V should contain at least $\lceil \log \left| \begin{bmatrix} V \\ 1 \end{bmatrix} \right| \rceil \geq (n-1) \log q$ subspaces. Note that if $q = 2$, then the formula gives $\lceil \log 2^n - 1 \rceil = n$ as lower bound.

We will describe two algorithms to show the upper bound $A(n,q) \leq (q-1)(n-1)+1$. The first algorithm is a very simple inductive one and generalizes the algorithm that we had in the projective plane case. First of all, note that if $n = 2$, then the bound to prove is q and just by asking q out of the $q+1$ possible 1-subspaces we can determine the unknown 1-subspace $\mathbf{u}$. Let us assume that for all $k < n$ we obtained an algorithm in the k dimensional space that uses only $(k-1)$-subspaces as queries.

Consider any $(n-2)$-subspace U of V. There are exactly $q+1$ $(n-1)$-subspaces $U_1, \ldots, U_{q+1}$ of V that contain U. Let us ask q of them. After getting the answers to these queries, we will know whether $\mathbf{u} \leqslant U$ or $\mathbf{u} \subset U_i \setminus U$ holds for some $1 \leq i \leq q+1$ and in the latter case we even know the value of i. If $\mathbf{u} \leqslant U$, then by induction we can finish our algorithm in $(n-3)(q-1)+1$ queries that gives a total of $(n-2)(q-1)+2$ queries. If $\mathbf{u} \subset U_i \setminus U$, then by our assumption that an algorithm for the $(n-1)$ dimensional case uses only $(n-2)$-spaces, we can assume that the first query is U and thus we need only $(n-2)(q-1)$ more queries giving a total of $(n-1)(q-1)+1$ queries. Note that we can also satisfy the assumption that we only use $(n-1)$-subspaces, since, instead of querying an $(n-2)$-subspace A of U_i, we can ask an $(n-1)$-subspace $A' \leqslant V$ such that $A' \cap U_i = A$.

Note that even this easy algorithm does not utilize the whole power of adaptiveness as when decreasing the dimension by one, we can ask the q queries at once. Thus the above algorithm uses at most $n-1$ rounds. In what follows, we introduce a two-round algorithm that uses the same number of queries to determine the unknown 1-subspace $\mathbf{u}$.

Before describing the two-round algorithm note that to determine a 1-subspace $\mathbf{u}$ it is enough to identify one non-zero vector $u \in \mathbf{u}$ as then $\mathbf{u} = \{\lambda u : \lambda \in \mathrm{GF}(q)\}$. In the next reasoning we will think of a vector $v \in V$ as an n-tuple of elements of $\mathrm{GF}(q)$. For $i = 1, 2, \ldots, n$ let us define the following $(n-1)$-subspaces of V: $A_i = \{v = (v_1, v_2, \ldots, v_n) \in V : v_i = 0\}$. Let $e_1, e_2, \ldots, e_n$ denote the standard basis of V and for $1 \leq i < j \leq n$ let us write $E_{i,j} = \langle e_i, e_j \rangle$. All $E_{i,j}$'s have dimension 2, therefore each of them contains $q+1$ 1-subspaces. Two of those are $\{v = (v_1, v_2, \ldots, v_n) \in E_{i,j} : v_i = 0\}$ and $\{v = (v_1, v_2, \ldots, v_n) \in E_{i,j} : v_j = 0\}$. For every pair i, j let $\mathbf{l}_{i,j,1}, \mathbf{l}_{i,j,2}, \ldots, \mathbf{l}_{i,j,q-1}$ be an arbitrary enumeration of the $q-1$ other 1-subspaces of $E_{i,j}$. Finally, for any $1 \leq i < j \leq n$ and $1 \leq k \leq q-1$ let us write $L_{i,j,k} = \{v = (v_1, v_2, \ldots, v_n) \in V : (0, \ldots, 0, v_i, 0, \ldots, 0, v_j, 0, \ldots, 0) \in \mathbf{l}_{i,j,k}\}$. Clearly, all $L_{i,j,k}$'s are $(n-1)$-subspaces of V.

In the first round, our algorithm asks all subspaces A_i, $i = 1, 2, \ldots, n$ as queries. Let Z

and NZ denote the set of coordinates for which the answer was YES and NO, respectively. (Note that if $q = 2$, then we are done as with the answers to the queries of the first round we will be able to tell the one and only non-zero vector u of $\mathbf{u}$. This gives an algorithm of n queries that matches the trivial lower bound mentioned earlier.) Let T be any tree with vertex set NZ. Then in a second round of queries our algorithm asks the subspaces $L_{i,j,k}$ with $(i,j) \in E(T)$ and $1 \leq k \leq q-2$. We claim that after obtaining the answers to these queries, we are able to identify a vector $0 \neq u = (u_1, u_2, \ldots, u_n) \in \mathbf{u}$. Clearly, we have $u_i = 0$ if and only $i \in Z$. As for any $i \in NZ$, we have $u_i \neq 0$, we obtain that for any pair $i, j \in NZ$ we have $(0, \ldots, 0, u_i, 0, \ldots, 0, u_j, \ldots, 0) \in \mathbf{l}_{i,j,k}$ for some $1 \leq k \leq q-1$. Thus by our queries of the second round, we will be able to tell to which such 1-subspace of $E_{i,j}$ the vector $(0, , , 0, u_i, 0, \ldots, 0, u_j, \ldots, 0)$ belongs.

Let us pick an arbitrary coordinate $x \in NZ$. We may assume that $u_x = 1$ as if not, then we can consider $u_x^{-1}u$ instead of u. Now for any $j \in NZ$ with $(x,j) \in E(T)$ we can find out u_j as there is exactly one vector in $\mathbf{l}_{x,j,k}$ with x-coordinate 1. As T is connected and contains all coordinates from NZ, we can determine all u_i's with $i \in NZ$ one by one. □

One may obtain a bound in the non-adaptive case using a very similar strategy to that in the 2-round proof of Theorem 6.3. As this time we have to ask all queries at a time, we have to make sure that no matter what NZ turns out to be we ask queries according to the edges of a connected graph on NZ. To this end we do not have any other choice than to query for all pairs $1 \leq i < j \leq n$. That is, we ask the separating system of the following subspaces:

$$\{A_i : i = 1, 2, \ldots, n\} \cup \{L_{i,j,k} : 1 \leq i < j \leq n, 1 \leq k \leq q-2\}.$$

A proof identical to that in the adaptive case shows that this set of subspaces form a separating system. This shows the bound $M(n,q) \leq n + \binom{n}{2}(q-2)$. Thus we obtain that if n is fixed, then $M(n,q)$ grows linearly in q. Our aim is not only to prove a similar statement for n, but to show that $M(n,q)$ grows linearly in nq. It is easy to see that the number of pairs of 1-subspaces separated by a subspace U is maximized when $\dim(U) = n-1$. Thus a natural idea is to consider a set of randomly picked $(n-1)$-subspaces as candidate for a separating system of small size. This would yield the upper bound $M(n,q) = O(nq \log q)$. Another idea is to generalize what we used in the case of projective planes. If $n = 3$, then the set of lines incident to at least one of 3 non-collinear points forms a separating system of size $3q-3$. Results of Section 6.2 show that this is not optimal, but is still of the right order of magnitude. Combining these two ideas, we obtain a proof of Theorem 6.4.

Theorem 6.4 (upper bound). $M(n,q) \leq 2q(n-1)$.

Proof. Let V be an n-dimensional vector space over GF(q) and let $X_1, X_2, \ldots, X_l$ be independent identically distributed random variables taking their values uniformly among all $(n-2)$-dimensional subspaces of V. For every X_i, there are exactly $q+1$ $(n-1)$-subspaces containing X_i, let us denote them by $X_{i,1}, X_{i,2}, \ldots, X_{i,q+1}$. For any pair $\mathbf{u}, \mathbf{v}$ of 1-subspaces of V, let $S_{\mathbf{u},\mathbf{v}}$ denote the indicator random variable of the event that $\mathbf{u}$ and $\mathbf{v}$ are not separated by $X_{1,1}, \ldots, X_{1,q}, X_{2,1}, \ldots, X_{2,q}, \ldots, X_{l,1}, \ldots, X_{l,q}$.

Claim. Let $\mathbf{u}$ and $\mathbf{v}$ be different 1-subspaces of V. Then the number of $(n-2)$-subspaces U of V such that the family $\{U_1, U_2, \ldots, U_{q+1}\}$ of all $(n-1)$-subspaces of V containing U does not separate $\mathbf{u}$ and $\mathbf{v}$ is $(q-1)\begin{bmatrix} n-1 \\ n-3 \end{bmatrix} - (q-2)\begin{bmatrix} n-2 \\ n-4 \end{bmatrix}$.

Proof of Claim. Clearly, if $\mathbf{u}, \mathbf{v} \in U$, then $U_1, U_2, \ldots, U_{q+1}$ do not separate $\mathbf{u}$ and $\mathbf{v}$, while if exactly one of them lies in U, then $U_1, U_2, \ldots, U_{q+1}$ do separate them. If $\mathbf{u}, \mathbf{v} \notin U$, then $\mathbf{u}$ and $\mathbf{v}$ are not separated by $U_1, U_2, \ldots, U_{q+1}$ if and only if $\dim(U, \langle \mathbf{u}, \mathbf{v} \rangle) = n-1$, that is if U meets $\langle \mathbf{u}, \mathbf{v} \rangle$ in a 1-subspace different from both $\mathbf{u}$ and $\mathbf{v}$. As there are $q-1$ such 1-subspaces, the number of such U's is $(q-1)\left(\begin{bmatrix} n-1 \\ n-3 \end{bmatrix} - \begin{bmatrix} n-2 \\ n-4 \end{bmatrix}\right)$. Thus the number of $(n-2)$-subspaces satisfying the condition of the claim is $\begin{bmatrix} n-2 \\ n-4 \end{bmatrix} + (q-1)\left(\begin{bmatrix} n-1 \\ n-3 \end{bmatrix} - \begin{bmatrix} n-2 \\ n-4 \end{bmatrix}\right)$ as claimed. ■

By the above claim we obtain the expected value of $S_{\mathbf{u},\mathbf{v}}$ satisfies

$$\mathbb{E}(S_{\mathbf{u},\mathbf{v}}) = \left(\frac{(q-1)\begin{bmatrix} n-1 \\ 2 \end{bmatrix} - (q-2)\begin{bmatrix} n-2 \\ 2 \end{bmatrix}}{\begin{bmatrix} n \\ 2 \end{bmatrix}} \right)^l \leq \left(\frac{(q-1)(q^{n-2}-1)}{q^n - 1} \right)^l \leq \frac{1}{q^l}.$$

And thus if we set $l = 2(n-1)$, then we have

$$\mathbb{E}(\sum_{\mathbf{u},\mathbf{v}} S_{\mathbf{u},\mathbf{v}}) \leq \begin{pmatrix} \begin{bmatrix} n \\ 1 \end{bmatrix} \\ 2 \end{pmatrix} \frac{1}{q^l} \leq 1/2.$$

Therefore, there exists a collection of $2(n-1)$ $(n-2)$-dimensional subspaces such that the set of $(n-1)$-dimensional subspaces containing any of them is a separating family. Clearly, to separate pairs of 1-subspaces, it is enough to query q of the $q+1$ $(n-1)$-subspaces containing a fixed $(n-2)$-subspace, and thus we have $M(n,q) \leq 2(n-1)q$. □

To obtain the lower bound in Theorem 6.4 we will use the following theorem of Katona [38] about separating systems of sub*sets* of an underlying set.

Theorem 6.11 (Katona [38]). *Let X be an M-element set and $\mathcal{A} \subseteq 2^X$ be a separating system of subsets of X such that for all $A \in \mathcal{A}$ we have $|A| \leq m$ for some integer $m < M/2$. Then the following inequality holds*

$$|\mathcal{A}| \geq \frac{\log M}{\log e\frac{M}{m}} \frac{M}{m}.$$

Theorem 6.4 (lower bound). *There exists an absolute constant $C > 0$ such that for any positive integer n and prime power q the inequality $\frac{1}{C}q(n-1) \leq M(n,q)$ holds. Moreover, if q tends to infinity, then $(1-o(1))q(n-1) \leq M(n,q)$ holds.*

Proof. Theorem 6.11 can be applied to obtain the desired bound. Indeed, as mentioned in the Introduction, if X is the set of all 1-subspaces of V and the set Q of all allowed queries is

$$\left\{ F \subset \begin{bmatrix} V \\ 1 \end{bmatrix} : \exists U \leq V \text{ with } F = \left\{ \mathbf{u} \in \begin{bmatrix} V \\ 1 \end{bmatrix} : \mathbf{u} \leq U \right\} \right\},$$

then we can write $M = \begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{q^n-1}{q-1}$ and $m = \begin{bmatrix} n-1 \\ 1 \end{bmatrix} = \frac{q^{n-1}-1}{q-1}$ since the largest "meaningful" query sets are those corresponding to $(n-1)$-subspaces of V. Substituting these values to the formula of Theorem 6.11 we obtain

$$M(n,q) \geq \frac{\log M}{\log e\frac{M}{m}} \frac{M}{m} = \frac{\log \frac{q^n-1}{q-1}}{\log e\frac{q^n-1}{q^{n-1}-1}} \frac{q^n-1}{q^{n-1}-1} \geq (n-1)q \frac{\log q}{2+\log \frac{q^n-1}{q^{n-1}-1}}.$$

□

6.4 Remarks

We may formulate the dual searching problem: a hyperplane H_0 of $\mathrm{PG}(n-1,q)$ is marked, and we can ask whether a subspace H is contained in H_0; how many queries do we need to identify H_0? Let us consider now the non-adaptive case in $\mathrm{PG}(n,q)$. Suppose that we only ask points as queries. Thus we are to find a point set S such that its intersection with any hyperplane is unique. Clearly, if the intersection of S and any hyperplane contains n points in general position, we are done. Note that, however, this condition implies that any hyperplane is generated by its intersection with S, which is clearly stronger than our original goal. Such a point set may be called a *hyperplane generating set*. Let us denote the size of the smallest hyperplane generating set by $\sigma(\mathrm{PG}(n,q))$, and denote the size of the smallest n-fold blocking set with respect to hyperplanes by $\tau_n^{n-1}(\mathrm{PG}(n,q))$. In case of $n=3$, that is projective planes, a hyperplane (line) generating set is just a double blocking set, thus $\sigma(\mathrm{PG}(2,q)) = \tau_2^1(\mathrm{PG}(2,q)) = \tau_2(\mathrm{PG}(2,q))$; furthermore, as seen in the remark after Theorem 6.10, $M(3,q)$ is usually a bit smaller than $\tau_2(\mathrm{PG}(2,q))$.

In higher dimensions an n-fold blocking set with respect to hyperplanes is not necessarily a hyperplane generating set. Trivially, $\tau_n^{n-1}(\mathrm{PG}(n,q)) \leq \sigma(\mathrm{PG}(n,q))$ and $M(n+1,q) \leq \sigma(\mathrm{PG}(n,q))$, but it is not clear how far these parameters are from each other if $n \geq 3$.

As any line intersects every hyperplane in at least one point, the union of n pairwise nonintersecting lines is an n-fold blocking set with respect to hyperplanes. We may also try

to find a hyperplane generating set as the union of some lines. Let us say that a set of lines is in *higgledy-piggledy position* if their union is a hyperplane generating set.

Thus if we could find a set of $h(n,q)$ lines in higgledy-piggledy position in $\mathrm{PG}(n,q)$, then $M(n+1,q) \leq h(n,q)q$ would follow. For $n=2$, any three non-concurrent lines suffice; for $n=3$, one may take three lines of the same regulus of a hyperbolic quadric and a fourth line disjoint from the quadric; for $n=4$, five lines turn out not to be enough [32]. For $n \geq 4$, we could not construct a small set of lines in higgledy-piggledy position so far. The arising questions seem quite interesting. These considerations led to further research, which was done by Fancsali and Sziklai in [31].

Bibliography

[1] P. Sziklai, M. Takáts, Vandermonde sets and super-Vandermonde sets. *Finite Fields Appl.*, **14** (2008), 1056–1067.

[2] P. Sziklai, M. Takáts, An extension of the direction problem. *Discrete Math.*, **312** (2012), 2083–2087.

[3] Sz. L. Fancsali, P. Sziklai, M. Takáts, The number of directions determined by less than q points. *J. Alg. Comb.*, Volume **37**, Issue **1** (2013), 27–37.

[4] J. De Beule, P. Sziklai, M. Takáts, On the structure of the directions not determined by a large affine point set. *J. Alg. Comb.*, Volume **38**, Issue **4** (2013), 888-899.

[5] T. Héger, M. Takáts, Resolving sets and semi-resolving sets in finite projective planes. *Electronic J. of Comb.*, Volume **19**, Issue 4 (2012).

[6] T. Héger, B. Patkós, M. Takáts, Search problems in vector spaces. *Designs, Codes and Cryptography*,(2014), DOI: 10.1007/s10623-014-9941-9.

[7] G. Bacsó, T. Héger, T. Szőnyi, The 2-blocking number and the upper chromatic number of PG$(2, q)$. *J. Comb. Des.*, to appear.

[8] R. F. Bailey, Resolving sets for incidence graphs. *Session talk at the 23rd British Combinatorial Conference*, Exeter, 5th July 2011.

[9] R. F. Bailey, P. J. Cameron, Base size, metric dimension and other invariants of groups and graphs. *Bull. London Math. Soc.*, **43** (2011), 209–242.

[10] S. Ball, Multiple blocking sets and arcs in finite planes. *J. London Math. Soc. (2)*, **54** no. 3 (1996), 581–593.

[11] S. Ball, The number of directions determined by a function over a finite field. *J. Combin. Th. Ser. A*, **104** (2003), 341–350.

[12] S. Ball, The polynomial method in Galois geometries. In: *Current research topics in Galois geometry*, Chapter 5, pages 103–128., Nova Sci. Publ., New York (2011).

[13] S. Ball, A. Blokhuis, On the size of a double blocking set in PG$(2, q)$. *Finite Fields Appl.*, **2** (1996), 125–137.

[14] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica*, **17**(1) (1997), 31–41.

[15] A. Blokhuis, S. Ball, A. Brouwer, L. Storme, T. Szőnyi, On the number of slopes determined by a function on a finite field. *J. Comb. Theory Ser. (A)*, **86** (1999), 187–196.

[16] A. Blokhuis, A. E. Brouwer, Blocking sets in Desarguesian projective planes. *Bull. London Math. Soc.* **18** no. 2 (1986), 132–134.

[17] A. Blokhuis, L. Storme, T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc. (2)*, **60** (1999), no. 2, 321–332.

[18] R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math.*, **13** (1963), 389–419.

[19] K. Coolsaet, J. De Beule, A. Siciliano, The known maximal partial ovoids of size $q^2 - 1$ of Q$(4, q)$. *J. Combin. Des.*, DOI: 10.1002/jcd.21307 (2012).

[20] A. Cossu, Su alcune proprietà dei $\{k, n\}$-archi di un piano proiettivo sopra un corpo finito. *Rend. Mat. e Appl. (5)*, **20** (1961), 271–277.

[21] J. De Beule, On large maximal partial ovoids of the parabolic quadric Q$(4, q)$. *Des. Codes Cryptogr.*, DOI: 10.1007/s10623-012-9629-y (2012).

[22] J. De Beule, A. Gács, Complete arcs on the parabolic quadric Q$(4, q)$. *Finite Fields Appl.*, **14**(1) (2008), 14–21.

[23] J. De Beule, A. Klein, K. Metsch, Substructures of finite classical polar spaces. In: *Current research topics in Galois geometry*, Mathematics Research Developments (editors: J. De Beule and L. Storme), Chapter 2, pages 35–61., Nova Sci. Publ., New York (2012).

[24] F. De Clerck, A. Del Fra, D. Ghinelli, Pointsets in partial geometries. In: *Advances in finite geometries and designs (Chelwood Gate, 1990)*, Oxford Sci. Publ., pages 93–110., Oxford Univ. Press, New York (1991).

[25] F. De Clerck, N. Durante, Constructions and characterizations of classical sets in PG(n, q). In: *Current research topics in Galois geometry*, Mathematics Research Developments (editors: J. De Beule and L. Storme), Chapter 1, pages 1–33., Nova Sci. Publ., New York (2012).

[26] F. De Clerck, H. Van Maldeghem, Some classes of rank 2 geometries. In: *Handbook of incidence geometry*, pages 433–475., North-Holland, Amsterdam (1995).

[27] S. De Winter, K. Thas, Bounds on partial ovoids and spreads in classical generalized quadrangles. *Innov. Incidence Geom.*, **11** (2010), 19–33.

[28] R. H. F. Denniston, Some maximal arcs in finite projective planes. *J. Combinatorial Theory*, **6** (1969), 317–319.

[29] D.-Z. Du, F.K. Hwang, *Combinatorial Group Testing and its Applications.* Series on Applied Mathematics (Singapore), 12. Singapore: World Scientific. xii, 323 p., 2nd ed. (English) (2000).

[30] Sz. L. Fancsali, Bounds and spectrum results in Galois geometry and coding theory. *Ph.D. thesis*, (2011).

[31] Sz. L. Fancsali, P. Sziklai, Lines in higgledy-piggledy position. *Submitted.*

[32] Sz. L. Fancsali, P. Sziklai, T. Szőnyi, Personal communication (2013).

[33] A. Gács, Zs. Weiner, On $(q + t, t)$-arcs of type $(0, 2, t)$. *Designs, Codes and Cryptography*, **29** (2003), 131–139.

[34] N. V. Harrach, Unique reducibility of multiple blocking sets. *J. Geometry* **103** (2012), 445–456.

[35] T. Héger, Some graph theoretic aspects of finite geometries *Ph.D. thesis*, (2013).

[36] J. W. P. Hirschfeld, *Projective geometries over finite fields.* Clarendon Press, Oxford (1979), 2nd edition (1998).

[37] J. W. P. Hirschfeld, J. A. Thas, *General Galois geometries.* Clarendon Press, Oxford (1991).

[38] G. Katona, On separating systems of a finite set. *J. Combin. Theory* **1** (1966), 174–194.

[39] Kiss Gy., Szőnyi T., *Véges geometriák.* Polygon, Szeged (2001).

[40] L. Lovász, A. Schrijver, Remarks on a theorem of Rédei. *Studia Scient Math. Hungar.* **16** (1981), 449–454.

[41] S. E. Payne, J. A. Thas, *Finite generalized quadrangles.* EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, second edition (2009).

[42] O. Polverino, Linear sets in finite projective spaces. *Discrete Math.*, **310**(22) (2010), 3096–3107.

[43] L. Rédei, *Lückenhafte Polynome über endlichen Körpern.* Birkhäuser Verlag, Basel (1970). English translation: *Lacunary polynomials over finite fields.* North Holland, Amsterdam (1973).

[44] B. Segre, Ovals in a finite projective plane. *Canad. J. Math.*, **7** (1955), 414–416.

[45] L. Storme, P. Sziklai, Linear point sets and Rédei type k-blocking sets in PG(n, q). *J. Alg. Comb.*, **14** (2001), 221–228.

[46] P. Sziklai, Polynomials in finite geometry. *Manuscript. Available online at* `http://www.cs.elte.hu/~sziklai/poly.html`

[47] P. Sziklai, On subsets of GF(q^2) with dth power differences. *Discrete Math.*, **208/209** (1999), 547–555. Combinatorics (Assisi, 1996).

[48] T. Szőnyi, A hézagos polinomok Rédei-féle elméletének néhány újabb alkalmazása. *Polygon*, **V.** kötet **2.** szám (1995).

[49] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane. *J. Combin. Theory Ser. A*, **74**(1) (1996), 141–146.

[50] T. Szőnyi, Around Rédei's theorem. *Discrete Math.*, **208/209** (1999), 557–575. Combinatorics (Assisi, 1996).

[51] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes. *Finite Fields and Appl.* **3** (1997), 187–202.

In the thesis we study geometries over finite fields (Galois-geometries), and "geometry style" properties of finite fields. The two main ways of finite geometrical investigations are the combinatorial and the algebraic one, there are examples for both methods in the thesis. In the second case we take a point set and translate its "nice" combinatorial property to a "nice" algebraic structure. In the thesis we mainly use the so-called polynomial method, developed by Blokhuis and Szőnyi.

The main part of the thesis is related to the *direction problem*. We say a point d at infinity is a *direction*, *determined* by an affine point set, if there is an affine line with the ideal point d containing at least two points of the set. The investigated questions are the *number* of determined directions, and the *size* and the *structure* of sets with few determined directions. In Chapter 2 we give some results on the number of determined directions by a small point set in the plane. In Chapter 3 we examine a stability question in n dimensions: can we extend a point set to a set of maximal cardinality such that the set of the determined directions remains the same. We show that if the set has almost maximal size then it is typically extendable. If not, then the set of non-determined directions has a strong structure. In Chapter 4 we generalize the original problem such that we define *determined k-dimensional subspaces* of the hyperplane at infinity. The studied questions arise from the classical problem. We classify point sets of maximal size in 3 dimensions, and describe the hierarchy of determined subspaces in n dimensions.

A set of size t is called *Vandermonde set* if at least the first $t-2$ power sums of its elements are 0, and it is called *super-Vandermonde set* if the $(t-1)$-th power sum vanishes as well, (these are extremal properties). The additive and multiplicative subgroups of the field $\mathrm{GF}(q)$ are natural examples, and there also exist geometrical examples: many interesting point sets can be translated to Vandermonde sets. In Chapter 1 we characterize "small" and "large" super-Vandermonde sets.

The last two chapters show some connections between finite geometries and other areas in combinatorics. A subset of the vertices of a simple graph is called *resolving set*, if for each vertex its ordered distance list with respect to this given subset is unique. The *metric dimension* of the graph is the size of its smallest resolving set. In Chapter 5 we give the metric dimension of the incidence graph of a finite projective plane and classify the smallest resolving sets. In Chapter 6 we consider a q-analog of the combinatorial search problem: our aim is to determine the minimum number of queries that is necessary to find a marked 1-dimensional subspace in an n-dimensional vectorspace, provided all queries are subspaces of the vectorspace and an answer says whether the marked subspace is contained in the subspace in question. We show that differently from the classical search problem, the minimum numbers of queries are not the same in the adaptive and in the non-adaptive case.

A disszertáció az algebra és a geometria egy határterületével, véges testre épített, azaz Galois-geometriákkal, illetve véges testek ,,geometriai jellegű" tulajdonságaival foglalkozik. A véges geometriai kérdéseknek kétféle szokásos tárgyalási módja a kombinatorikus és az algebrai, a dolgozatban mindkettőre látunk példákat. Utóbbinál azt vizsgáljuk, hogy egy ponthalmaz definiáló kombinatorikus, ,,szép" tulajdonsága lefordítható-e valamilyen ,,szép" algebrai struktúrává. Az egyik legfontosabb alkalmazott eszköz a Blokhuis és Szőnyi által megalkotott, azóta pedig sokak által továbbfejlesztett, ún. polinom-módszer.

A disszertáció döntő részében az *iránypróbléma* néhány lehetséges megközelítésével, illetve általánosításával foglalkozunk. Egy affin ponthalmaz által *meghatározott irány*nak nevezzük a d végtelen távoli pontot, ha van olyan affin egyenes, melynek ideális pontja d, és legalább 2 pontban metszi a halmazt. Kérdés a meghatározott irányok *száma*, illetve a *kevés* irányt meghatározó ponthalmazok *mérete*, *struktúrája*. A 2. fejezetben kis méretű, síkbeli ponthalmazok esetén adunk a meghatározott irányok számára vonatkozó részeredményeket. A 3. fejezetben n dimenzióban vizsgálunk egy stabilitási kérdést: egy ponthalmaz kiegészíthető-e maximális méretűvé úgy, hogy ne határozzon meg új irányt. Megmutatjuk, hogy ha a maximális mérettől való eltérés kicsi, akkor a ponthalmaz tipikusan kiegészíthető, illetve ha nem, akkor a meg nem határozott irányok halmaza erős struktúrával bír. Az eredeti definíciót kiterjeszthetjük a végtelen távoli hipersík *meghatározott k dimenziós altereire*. A vizsgált kérdések hasonlóak, mint a klasszikus problémánál. A 4. fejezetben 3 dimenzióban klasszifikáljuk a maximális méretű ponthalmazokat, illetve n dimenzióban vizsgáljuk a meghatározott alterek hierarchiáját.

Egy t méretű halmaz *Vandermonde-halmaz*, ha elemeinek legalább az első $t-2$ hatványösszege 0, és *szuper-Vandermonde-halmaz*, ha a $(t-1)$. hatványösszeg is 0. (Ezek extremális tulajdonságok.) Kézenfekvő példa $\mathrm{GF}(q)$ bármely additív vagy multiplikatív részcsoportja, de számos, geometriailag érdekes ponthalmazból is természetes módon kaphatunk Vandermonde-halmazokat. Az 1. fejezetben leírjuk a ,,kis" és ,,nagy" méretű szuper-Vandermonde-halmazokat.

Az utolsó két fejezet kitekintés a véges geometria más kombinatorikai területekkel való kapcsolatára. Egy egyszerű gráfban a csúcsok egy részhalmaza *megoldóhalmaz*, ha az ezen részhalmaz csúcsaitól vett távolságok rendezett listája a gráf minden csúcsára különböző. A legkisebb megoldóhalmaz mérete a gráf *metrikus dimenziója*. Az 5. fejezetben megadjuk véges projektív síkok incidenciagráfjának metrikus dimenzióját, valamint klasszifikáljuk a legkisebb megoldóhalmazokat. A 6. fejezetben a klasszikus kombinatorikus keresési probléma egy q-analógját vizsgáljuk: célunk n dimenziós vektortérben egy 1 dimenziós altér megtalálásához szükséges és elegendő minimális kérdésszám meghatározása, ha a kérdések a vektortér alterei, és egy válasz megadja, hogy az adott altér tartalmazza-e a keresett 1 dimenziós alteret. Megmutatjuk, hogy a klasszikus problémától eltérően az adaptív és a nem adaptív esetben a minimális kérdésszám különbözik.